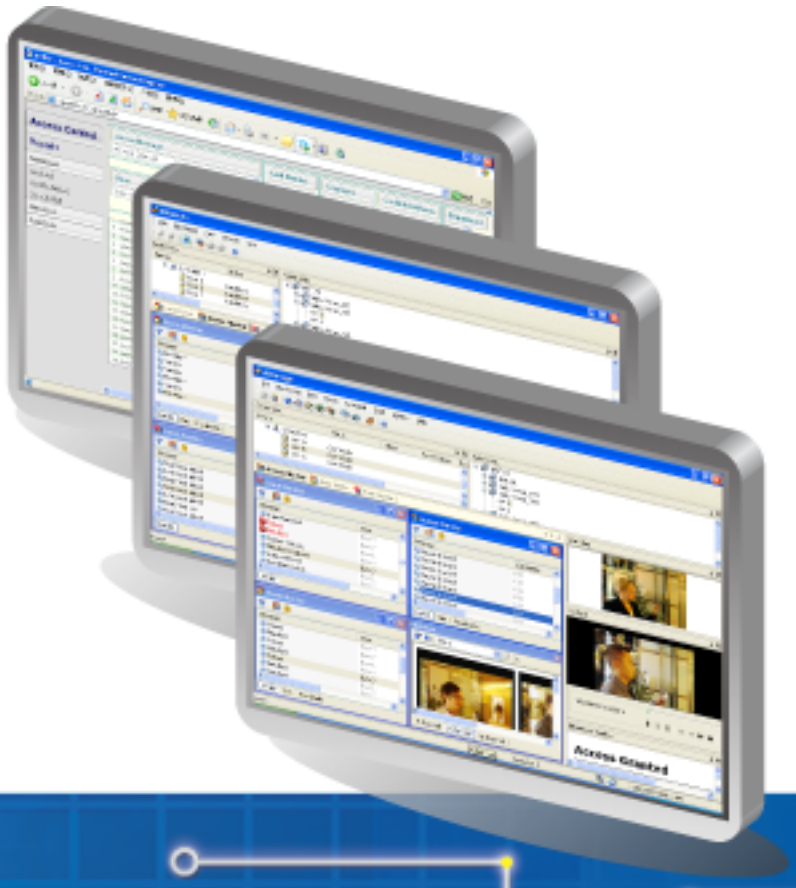
GeoVision inc
The Vision of Security

# GV-ASManager

## User's Manual V2.1.1





Every effort has been made to ensure that the information in this manual is accurate. GeoVision is not responsible for printing or clerical errors.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw



October 2009

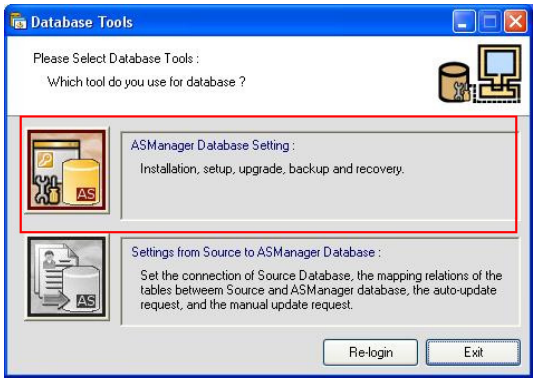
# Contents

# Note for the User of Upgrading GV-ASManager

You can keep your current database and upgrade it to work with GV-ASManager version 2.1. Follow the steps below to back up the database of version 2.0 and restore it to the GV-ASManager of version 2.1.

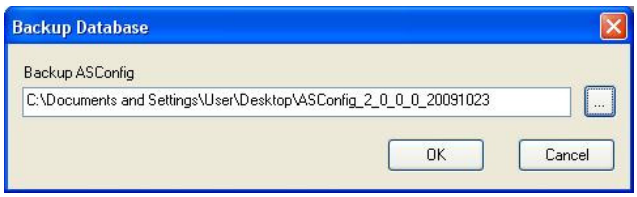
## Backing up the Database of Version 2.0

1. Run **ASDBManager.exe** from the V2.0 program folder at **:\AS200\ASManager**.
2. Select **ASManager Database Setting**.




3. Select **ASManager Database Backup**.

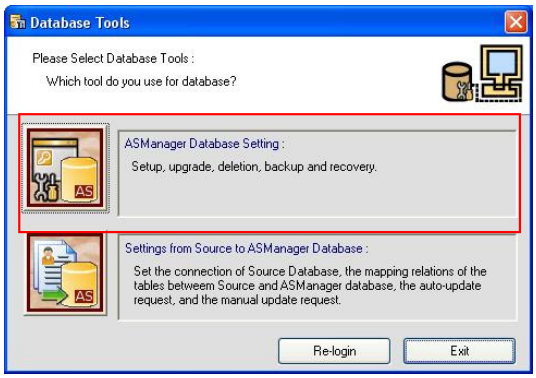

4. Specify a location to save the backup file, and click **OK**.



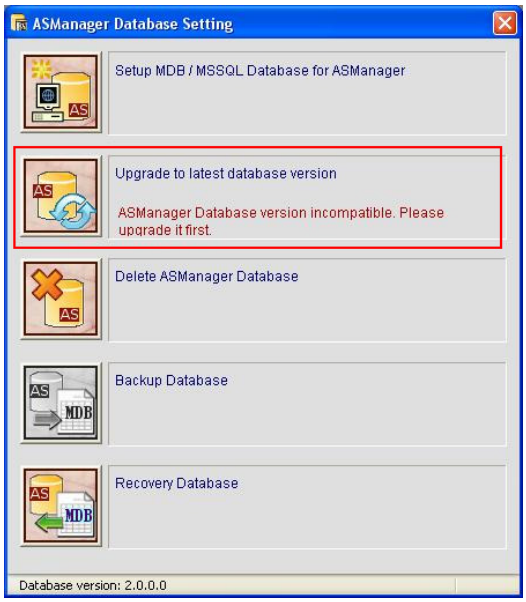

5. When the backup is complete and the message “Backup database successfully” appears, click **OK** and close all open dialog boxes.

## Installing GV-ASManager V2.1 and Restoring the Database V2.0

1. Uninstall **GV-ASManager V2.0** before installing the new version.
2. Install **GV-ASManager V2.1**.
3. Run **ASDBManager.exe** from the V2.1 program folder at **:\Access Control\ASManager**.
4. Select **ASManager Database Setting**.

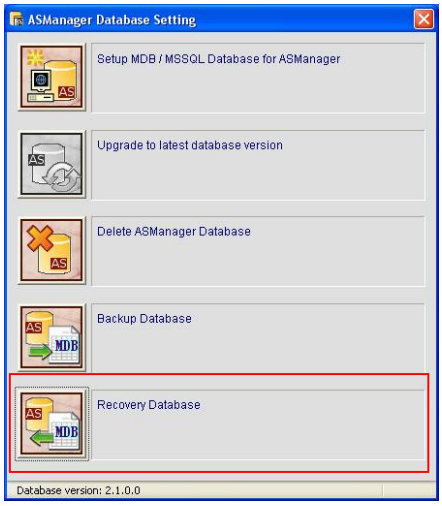



5. Select **Upgrade to latest database version**.

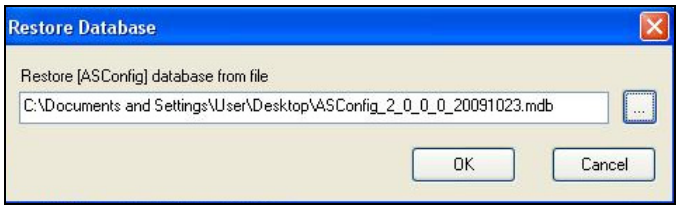



6. The GV-ASManager starts upgrading the database. When the upgrade is complete and the message “Upgrade database successfully” appears, click **OK**.

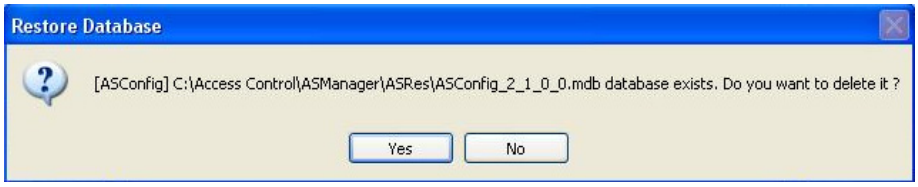
7. To restore the database of version 2.0, select **Recovery Database**.



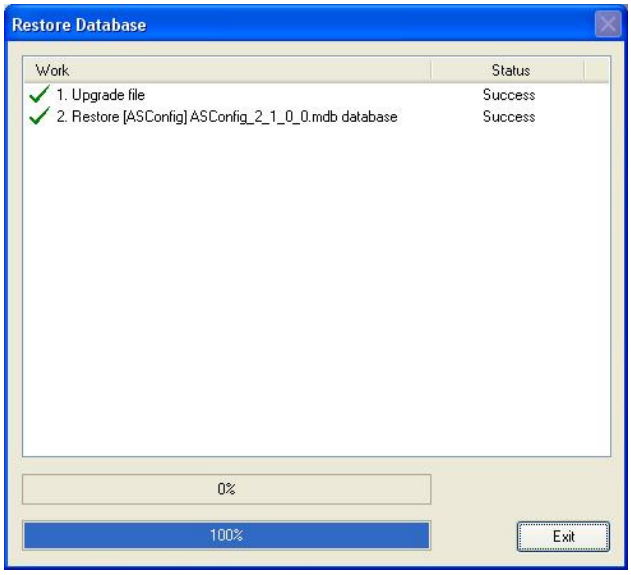

8. Specify the location of the backup database, and click **OK**.




9. When a warning message of the existence of the V2.1 database appears, select **Yes**.



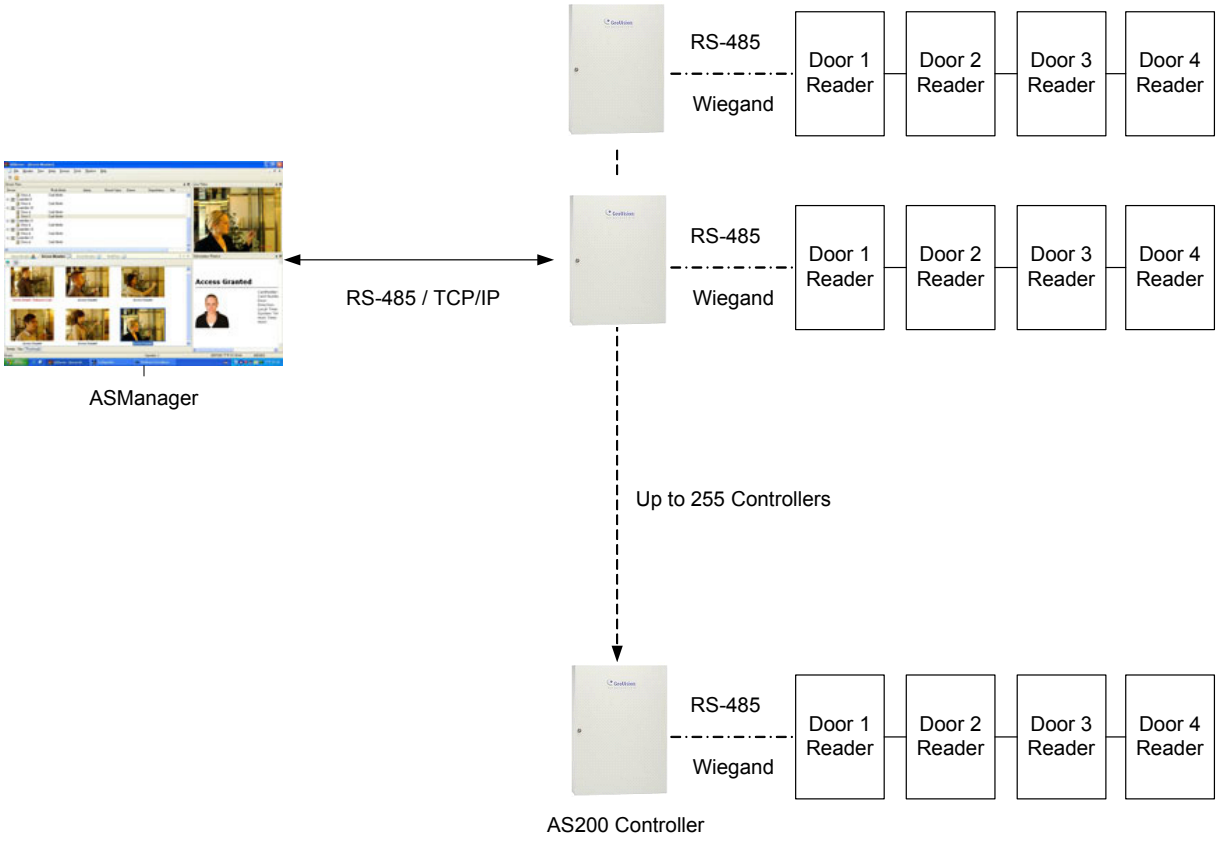

10. The GV-ASManager starts to restore the database of version 2.0 and convert it to version 2.1.



# Chapter 1 Introduction

The GV-ASManager and GV-AS Controller are the combination that offers the full control of the entrances of your premise. Up to 255 units of GV-AS Controllers can be monitored and controlled by one GV-ASManager.

The following diagram is an example of how the GV-ASManager and GV-AS Controller can be set up.



## 1.1 Main Features

### GV-ASManager

- Control up to 255 GV-AS Controllers
- Up to 256 time zones and weekly schedules
- Up to 10,000 cards (GV-AS200). Up to 40,000 cards (GV-AS100 and GV-AS400)
- Up to 1,000 system users
- Holiday planning for 14 months
- Multiple cards per user
- Four (4) access mode options: Card only mode (default), Card and PIN Code mode, Card or Common mode, Release mode
- Enroll cards in batch mode
- Door alarms: door held open, door forced entry, tamper, access denied
- Duress operation
- Anti-Passback capabilities
- Man trap in double door configuration
- Import/export of card and cardholder data in Access or Excel file format
- User-defined matrix of 16-channel multi-views
- User-defined screen layout and dual monitor display support
- SMS or E-Mail notification with user-defined content, video snapshot and cardholder photo
- Video integration with GeoVision IP devices (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR, GV-IP Camera) and third-party IP cameras
- Support Microsoft Access or SQL database

### GV-ASLog

- Log information with corresponding video and snapshot

### GV-ASRemote

- Monitor unlimited GV-ASManagers over the Internet
- Remote door monitoring, video playback, door operation

### GV-ASWeb

- Web interface for historical log search with corresponding video and snapshot
- Log export in Excel, Text, HTML file formats

## 1.2 Concepts

Understanding the following concepts may help you read through the manual.

| | |
|---|---|
| **Weekly Schedule** | A weekly schedule is certain days of the week when a user is granted access to a secure site.<br>For details, see *4.4 Setting Weekly Schedule.* |
| **Access Group** | An access group is a group of cardholders with identical location restrictions during the same time restraints.<br>For details, see *4.5 Setting Access Group.* |
| **Alarm Condition** | An alarm condition is a monitored condition through sensing devices, and an alarm condition may activate alarms. For example, the AS200 Controller has the ability to monitor 3 sensors, such as door status sensor, smoke detector and tamper detector. The AS200 Controller also provides 3 output relays for activating and deactivating electric lock, siren and emergency door release when the alarm condition occurs.<br>For settings of alarm conditions see *4.2.2 Step 2:Configuring a Door*. For configuring inputs and outputs see *GV-AS Controller Hardware Installation Guide.* |
| **Anti-Duress** | If a person is forced to open the door under threat, he can enter his PIN plus 1 to activate an alarm and send a signal to the ASManager to dispatch the police. For example, the PIN is 5555 and you enter 5556. The door will open normally (access granted) and the alarm will be activated. The function is enabled by default in the system. |
| **Anti-Passback** | The feature is designed to prevent card sharing and to enforce use of entry and exit readers. If a card was used at an entry reader, it must be used at an exit reader before it will be valid at an entry reader again.<br>For settings, see *4.2.2 Step 2:Configuring a Door*. |
| **Interlock** | The feature is also called “mantrap” or interlocking”. The feature interlocks two controlled doors allowing only one door to be opened at a time. The feature will not unlock a door if the other door is open. If both doors are open at the same time, the alarm will be activated.<br>For settings, see *4.2.1 Step 1: Configuring a Controller*. |

| | |
|---|---|
| **Two-person A/B rule** | The door unlock only when two assigned cards are presented together.<br>For settings, see *4.3.1 Adding a Single Card*. |
| **IP device** | The video device is connected to the ASManager through the network. The ASManager enables you to access the live video from not only GeoVision IP devices (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR and GV-IP Camera) but also certain third-party IP cameras.<br>For details, see *Chapter 5 Video Integration*. |

# Chapter 2 Installation

## 2.1 System Requirements

1. For GV-ASManager version 2.0 or later, the minimum hardware and software requirements are:

| | |
|---|---|
| OS | Windows 2000 / XP / Server 2003 / Vista |
| CPU | Pentium 4, 3.0 GHz with Hyper-Threading |
| Memory | 2 x 256 MB Dual Channels |
| Hard Disk | 2.0 GB |
| VGA | NVIDIA GeForce 7300 GT 128MB (PCI slot), or<br>ATI Radeon 9550 / 9600 / X1050 Series 256MB (AGP slot)<br>No support for onboard VGA |
| DirectX | End-User Runtimes (November 2008) |
| Software | .NET Framework 3.5<br>SQL Server 2005 Express (optional) |
| Browser | Internet Explorer 7.0 or later |
| **Note:** The software programs End-User Runtimes (November 2008) and .NET Framework 3.0 are necessary to run the GV-ASManager. The software programs can be found in the accompanying software CD. | |

- ASManager version 2.0 or later must work with **GV-AS200 Controller firmware version 1.0 or later**.

---

**Note:** .Net Framework cannot be installed on Windows 2000. See *2.2 Notes for Using Windows 2000*.

---

## 2.2 Notes for Using Windows 2000

If you run GV-ASManager on Windows 2000, please note these restrictions:

1. The Calendar System is not supported on Windows 2000 because **.Net Framework** cannot be installed on Windows 2000. For this feature, see *7.4 Calendar System.*
2. To connect GV-ASManager to SQL Server, it is required to install **Microsoft Data Access Components (MDAC) 2.8 SP1** from Software CD to the computer. For this feature, see *Chapter 11 Database Settings*.
3. The GV-ASLog and GV-ASWeb functions cannot work on Windows 2000 because these functions require **Internet Explorer 7** which is not supported by Windows 2000. For the two functions, see *Chapter 8 GV-ASLog* and *Chapter 10 GV-ASWeb*.
4. The Tiles tab is not available on the Alarm Monitor and Access Monitor windows. See *3.3 Monitoring Windows*.

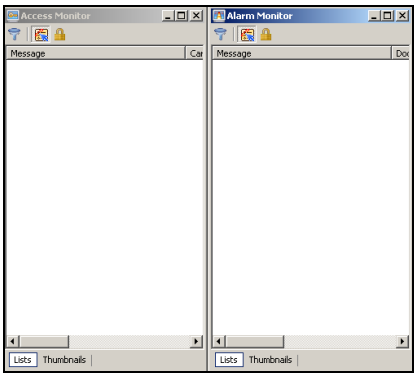



*Figure 2-1*

5. The Camera List is not available on the MultiView window. See *5.4 The MultiView Window.*

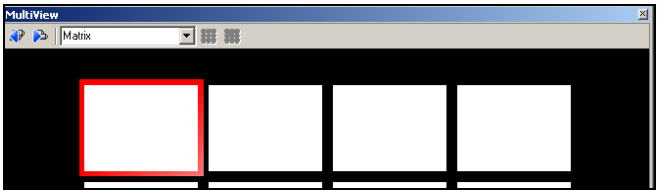



*Figure 2-2*

6. For the Live Video window and Playback window, the camera name displayed in the camera list will not be updated automatically after the camera name is modified. You need to select the corresponding camera on the Camera List window (No. 11, Figure 3-1) to update the camera name manually. See *5.2.1 Live Video Window* and *5.5 Retrieving Recorded Video*.

## 2.3 Installing the GV-ASManager

Starting from version 2.0.1, the GV-ASManager software coming with GV-AS Controller can manage one controller. If you need to manage more than one controller, it is necessary to use the USB dongle with the GV-ASManager software. The available types of dongles for purchase are as follows:

- **Dongle 4** is used for connection of up to 4 GV-AS Controllers.
- **Dongle 10** is used for connection of up to 10 GV-AS Controllers.
- **Dongle 30** is used for connection of up to 30 GV-AS Controllers.
- **Dongle 50** is used for connection of up to 50 GV-AS Controllers.
- **Dongle 255** is used for connection of up to 255 GV-AS Controllers.

### To install the USB Dongle drivers:

1. Insert the USB Dongle to your computer.
2. Insert Software CD to your computer and a window will pop up automatically. Select **Install or Remove GeoVision GV-Series Driver** and click **Install Geovision USB Devices Driver**.

### To install the GV-ASManager:

The **GV-ASManager V2.0 or later** must run with DirectX End-User Runtimes (November 2008) and .NET Framework. Follow these steps to install the programs.

1. Insert Software CD to your computer and a window will pop up automatically.
2. If you don't have DirectX 9.0c installed in your computer, select **Install DirectX 9.0c**
3. Select **Install DirectX End-User Runtimes (November 2008)**.
4. Select **Install Microsoft .NET Framework Version 3.5.**
5. Select **Install GeoVision V2.1.0.0 Access Control System**, click **GeoVision Access Control System** and follow on-screen instructions to complete the installation.

## 2.4 Logging in

Before using the GV-ASManager, you need to set the login ID and password, and create a database.

1. Click **Start**, point to **Programs**, select **Access Control** and click **ASManager**. When you start the system for the first time, the system will prompt you for a Supervisor ID and Password as below.


*Figure 2-3*

2. Enter a name you wish to be the Supervisor in the ID field. Finish the setup by entering Password, Password Confirmation and a Hint (optional) that would remind you of the password. The features available in the dialog box:
   - **Auto Login:** Allows auto login as the current user every time when the system is launched. For security purpose, this feature is only recommended for a single-user system.
   - **Allow removing password system:** Allows the user to remove the ID and password database from the system. It is recommended to check this option in case of password loss. For details, see the same option in Figure 7-1.
   -  **:** Click this icon to open the onscreen keyboard and enter the login information.
3. Click **OK**. The message "*Can't open database. Would you like to set up database?*" appears.

4. Select **Yes** to create a database. The ID and password you have configured in Step 1 are required to access the feature. Then this dialog box appears.

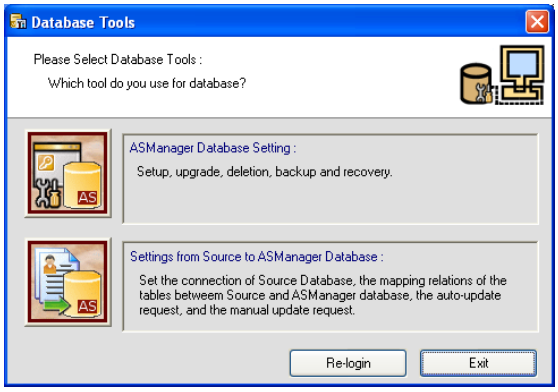



*Figure 2-4*

5. Select **ASManager Database Setting**. The ASManager Database Setting dialog box appears.
6. You can create either a Microsoft Access database or a Microsoft SQL database. To create a Microsoft SQL database, see *Chapter 11 Database Settings*. To create a Microsoft Access database:

   - **For the first-time user of GV-ASManager:**

   Select **Setup MDB / MSSQL Database for ASManager**. The Setup Database Connection dialog box appears. Select **Microsoft Office Access Database**, and click **OK**. The program starts creating a database. When it is complete, the message "*Setup database connection successfully*" will appear.

   - **For the user of upgrading GV-ASManager version to 2.1 or later:**

   Select **Upgrade to Latest Database Version**. The program starts upgrading the old database. When it is complete, the message "*Upgrade database successfully*" will appear.

7. Restart **ASManager**. You can see the main screen of the GV-ASManager.

---

**Note:**

1. After you upgrade GV-ASManager, it is recommended to also upgrade the GV-AS Controller firmware. To upgrade the controller firmware, use the **Update to the latest firmware version** function in the Net Module Utility. See *Chapter 12*.
2. By default the Access database is created at C:\Access Control\ASManager\ASRes.

---

# Chapter 3 The Main Screen of GV-ASManager

After you run the GV-ASManager, the following main screen will appear. Get yourself familiar with the main screen, as it will help you when you read further in the following sections.

## 3.1 Main Screen

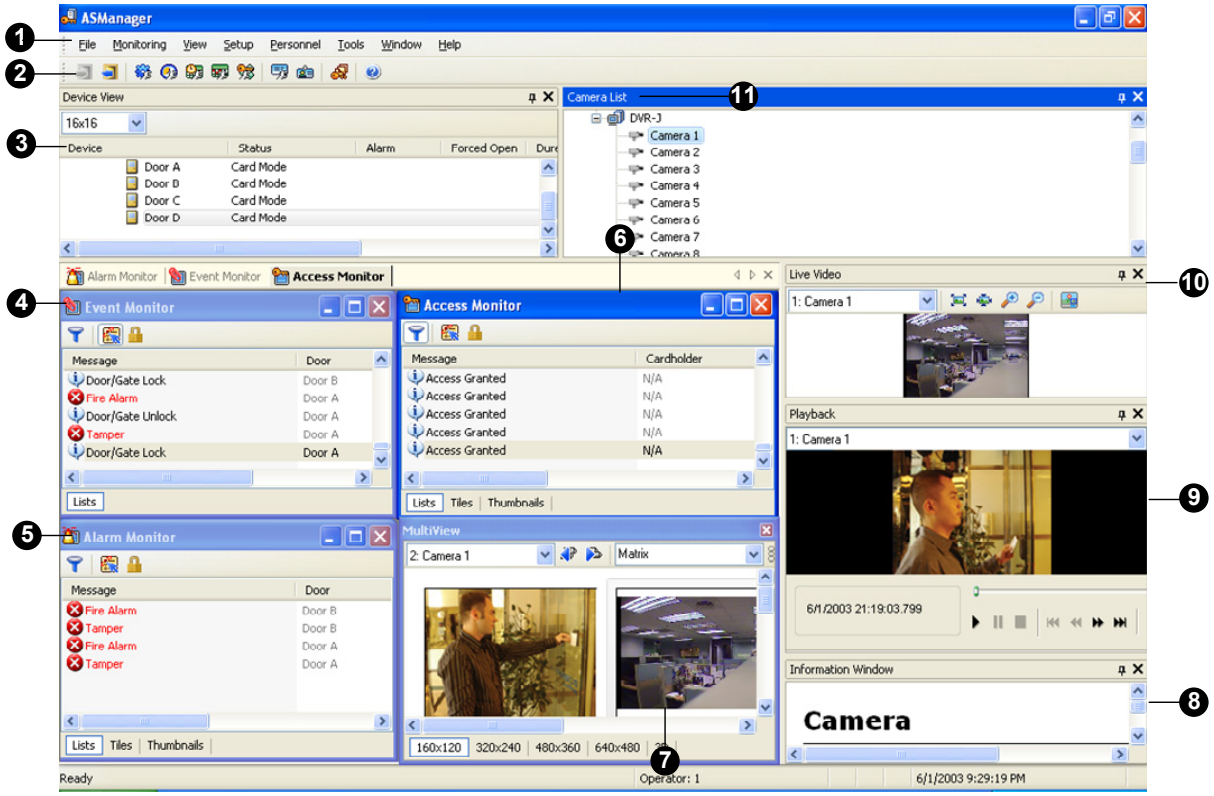



*Figure 3-1*

| No. | Name | Function |
|---|---|---|
| 1 | Menu Bar | The Menu Bar includes the options of **File** (log in / out the GV-ASManager), **Monitoring** (display monitor windows of alarm, access and event), **View** (display the function windows), **Setup** (set up connected devices and schedules), **Personnel** (set up the cardholders' accounts), **Tools** (set up for notification and log) and **Window** (arrange the display of different windows). |

| | | |
|---|---|---|
| 2 | Toolbar | The Toolbar includes the options of **Login**, **Logout**, **Devices**, **Time Zones**, **Weekly Schedules**, **Holidays**, **Access Groups**, **Cards**, **Cardholders**, **ASLog** and **About**. |
| 3 | Device View | Displays a list of connected doors and their current status. You can change the size of icons to 16 x 16, 24 x 24 or 32 x 32 from the drop-down list. |
| 4 | Event Monitor | Displays monitored events of doors. |
| 5 | Alarm Monitor | Displays alarm events of doors. |
| 6 | Access Monitor | Displays access activities of doors. |
| 7 | MultiView | Displays live views of connected cameras from multiple IP devices. For details, see *5.4 The MulitView Window*. |
| 8 | Information Window | Displays the information of doors, card readers and monitored events. |
| 9 | Playback | Plays back recorded events from a compatible GeoVision IP device. For details, see *5.5 Retrieving Recorded Video*. |
| 10 | Live Video | Displays the live view of one connected camera. For details, see *5.2 Accessing a Live View*. |
| 11 | Camera List | Displays a list of connected cameras. |

### 3.1.1 Toolbar

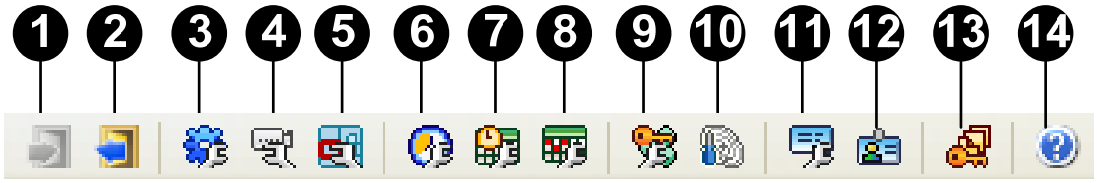



*Figure 3-2*

The buttons on the Toolbar of GV-ASManager:

| No. | Name | Function |
|---|---|---|
| 1 | Login | Logs in the GV-ASManager. |
| 2 | Logout | Logs out the GV-ASManager. |
| 3 | Devices | Defines controllers and doors. |

| | | |
|---|---|---|
| 4 | Cameras | Searches the GV IP devices on the same network. For details, see *Chapter 5 Video Integration*. |
| 5 | Areas | Configures Global Anti-Passback. For details, see *6.3 Global Anti-Passback.* |
| 6 | Time Zones | Defines the minutes and hours of the day when a user is granted access to a secure site. For details, see *4.4.1 Step 1:Setting Time Zones*. |
| 7 | Weekly Schedules | Defines the days of the week when a user is granted access to a secure site. For details, see *4.4.2 Step 2:Setting Weekly Schedules*. |
| 8 | Holidays | Defines the specific dates as holidays. For details, see *4.4.3 Step 3:Setting Holidays*. |
| 9 | Access Groups | Sets up different groups to define who can access what door at what time of a day. For details, see *4.5 Setting Access Groups*. |
| 10 | Fingerprint Access | Uploads the enrolled fingerprints to the controllers. For details, see *7.5.3 Uploading Fingerprints to Controllers*. |
| 11 | Cards | Creates and edits a database of card information. For details, see *4.3 Setting Cards*. |
| 12 | Cardholders | Creates and edits a database of cardholder information. For details, see *4.6 Setting Cardholders*. |
| 13 | ASLog | Displays the logs of access activities, alarm reports and monitored events. For details, see *Chapter 6 GV-ASLog*. |
| 14 | About | Displays the version of GV-ASManager. |

## 3.2 Device View

The Device View displays the activity and status of the connected doors.

- To open the Device View window, click **View** on the menu bar and select **Device View**.

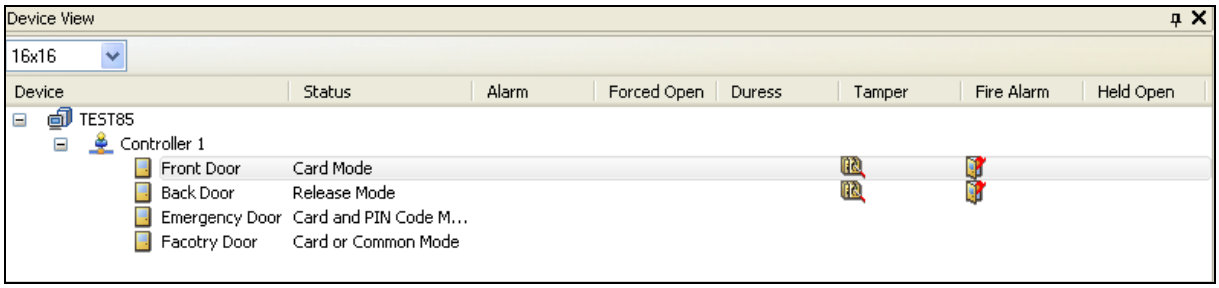



*Figure 3-3*

### 3.2.1 Controls on the Window

You can control a connected controller or door by right-clicking it in the Device View window.

The menu options of the **Host** include:

| Name | Function |
|---|---|
| Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation | Controls the behaviors of all doors associated with the server. |
| Reset Anti-Passback | Clicking this option enables a user to re-access the entry or exit reader.<br>See *Chapter 6 Anti-Passback*. |

The menu options of the **Controller** include:

| Name | Function |
|---|---|
| Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation | Controls the behaviors of all doors associated with the controller. |

| | |
|---|---|
| Reset Anti-Passback | Clicking this option enables a user to re-access the entry or exit reader.<br>See *Chapter 6 Anti-Passback*. |
| Reconnect | Reconnects with the controller. |
| Update | After the controller settings are modified, clicking Update can immediately renew the settings. |
| Settings | Modifies the controller settings in the Controller Setup dialog box. |

The menu options of the **Door** include:

| **Name** | **Function** |
|---|---|
| Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation | Controls door behaviors. |
| Clear Alarm, Clear Force Open, Clear Duress, Clear Tamper, Clear Fire Alarm, Clear Held Open, Clear Access Denied | Clears the alarm conditions.<br>For alarm settings, see Step 5 in *4.2.2 Step 2: Configuring a Door*. |
| Settings | Modifies the controller settings in the Controller Setup dialog box. |

**Note:**

1. The options of **Force Unlock** and **Force Lock** will let the door stay open or locked until you select **Disable Door Lock Operation**.
2. The **Unlock Door** option will let the door open temporarily until the specified time is expired. See “Lock Reset Time” at Step 2 in *4.2.2 Step 2: Configuring a Door*.
3. The **Clear Alarm** option refers to clear alarm sounds.

## 3.3 Monitoring Windows

Three monitoring windows are provided for users to oversee different types of door activities: Access Monitor, Alarm Monitor and Event Monitor.

- To open these windows, click **Monitoring** on the menu bar, and select the desired windows.

### 3.3.1 Controls on the Window

The three monitoring windows of Access Monitor, Alarm Monitor and Event Monitor have the same controls on the window.

We use the Access Monitor window as example to explain the controls.

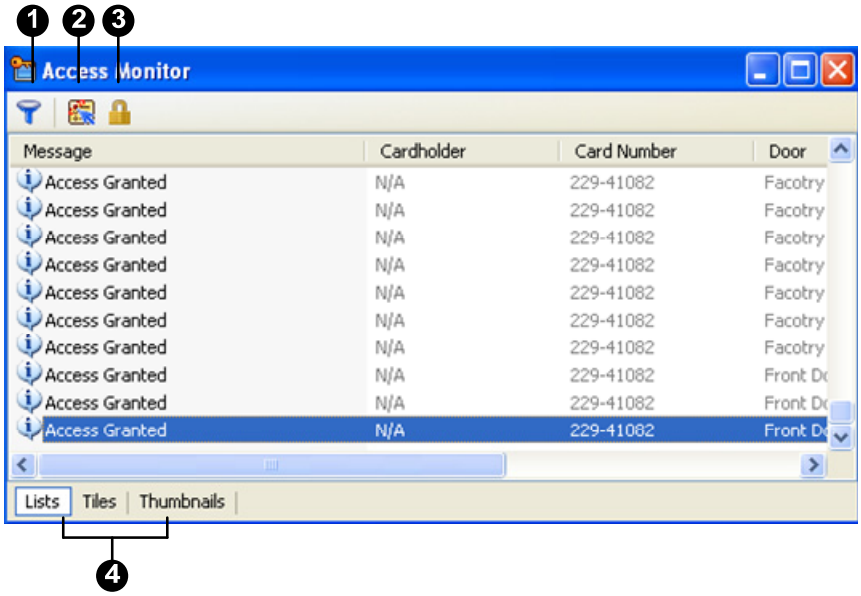



*Figure 3-4*

| No. | Name | Function |
|---|---|---|
| 1 | Filter | Sets up criteria to only display the desired activity information. |
| 2 | Auto Select | Focuses on the latest data display. |
| 3 | Lock | Suspends the current data display. |
| 4 | Lists / Tiles / Thumbnails | Decides how events are displayed on the window. For Windows 2000, the option of Tiles is not available on the Alarm Monitor and Access Monitor windows. |

The following options are only accessible on the **Access Monitor** window. Right-clicking one message allows you to access its detailed information.

| Name | Function |
|---|---|
| New/Edit Card | Enrolls a new card or edits the card information. |
| Browse Card Information | Views the card information. |
| Browse Cardholder Information | Views the cardholder information. |
| Show Image | If the camera monitors when the activity happened, the related image is available. |

### 3.3.2 Customizing a Monitoring Window

You can customize the messages displayed on a monitoring window by defining filter criteria. Multiple custom monitoring windows can be added for your specific requirements.

1. To add one monitoring window, click **Monitoring** on the menu bar. Then select **New Alarm Monitor**, **New Access Monitor** or **New Event Monitor**.
2. Click the **Filter** button on the monitoring window. This dialog box appears.

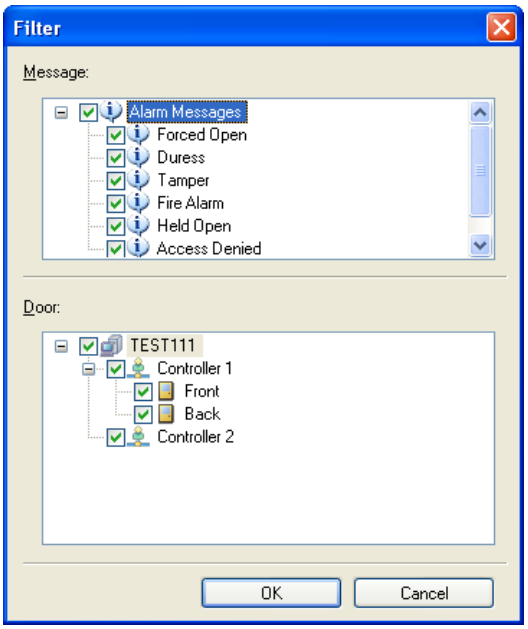



*Figure 3-5*

3. Select the desired messages and devices for monitoring, and click **OK**. The monitoring window will only display the messages based on the defined criteria.

4. Right-click the **Monitor** tab on the main screen, and select **Rename** to name the new monitoring window.

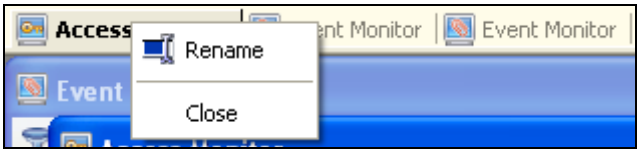



*Figure 3-6*

---

**Note:** The added windows are only for one-time use, and they cannot be saved after the monitoring window is closed.

---

### 3.3.3 Arranging Monitoring Windows

The monitoring windows can be arranged on screen in several ways.

On the menu bar, click **Window**, and select one of the following options to arrange the windows:

- **Cascade:** Overlaps the open windows and shows their title bars.
- **Tile Horizontally:** Arranges the open windows horizontally.
- **Tile Vertically:** Arranges the open windows vertically.
- **Arrange Icons:** Arranges the minimized windows on the bottom.

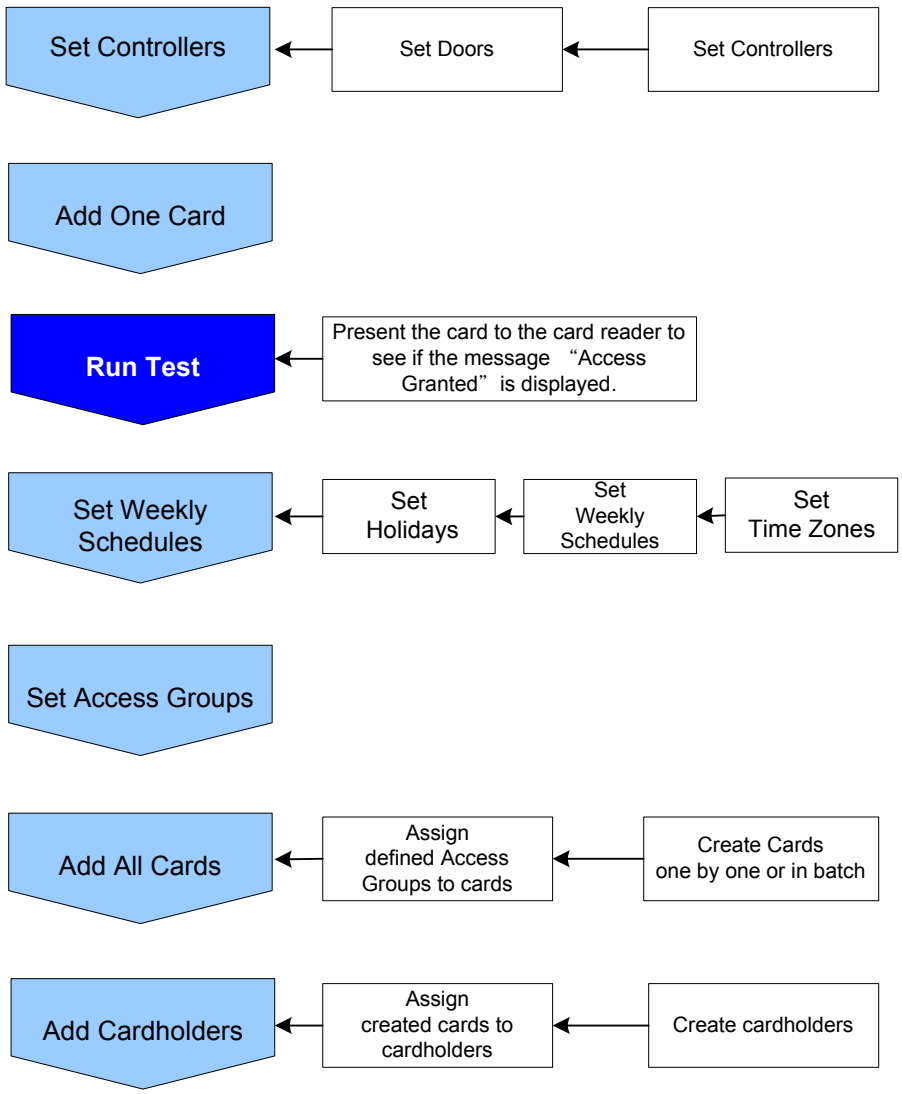
# Chapter 4 Settings

This section describes the following settings:

- Setting Controllers
- Setting Cards
- Setting Weekly Schedules
- Setting Access Groups
- Setting Cardholders

## 4.1 Setup Flowchart

To get started quickly with GV-ASManager settings, follow the process illustrated below.



## 4.2 Adding Controllers

To add the GV-AS Controller to the GV-ASManager, follow these steps:

- **Step 1 Configuring a Controller**

  Establish the communication between the GV-AS Controller and GV-ASManager.

- **Step 2 Configuring a Door**

  Define the doors on a door controller.

### 4.2.1 Step 1: Configuring a Controller

1. On the menu bar, click **Setup** and select **Device**. The Controller List dialog box appears.
2. Click the **Add** icon on the top left corner. This dialog box appears.

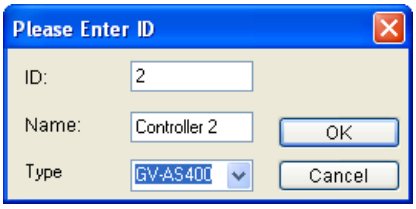



*Figure 4-1*

3. Enter **ID** and **Name** of the Controller, select **Type** of the Controller and click **OK**. This dialog box appears.

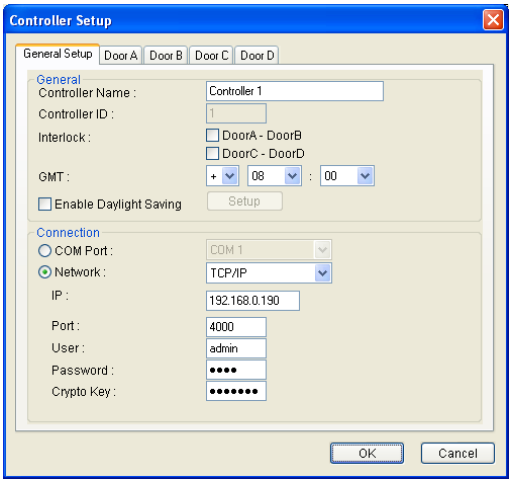



*Figure 4-2*

---

**Note:** The Controller ID is set ahead with GV-ASKeypad or Web interface. Refer to *GV-AS Controller Hardware Installation Guide*.

---

4. In Connection section, select the communication mode between the GV-AS Controller and GV-ASManager.
   - If using RS-485 connection, select **COM Port** that is used for connection.
   - If using Ethernet, select **Network** and select **TCP/IP** or **LocalDDNS**. Type the IP address, device name (if LocalDDNS is selected), port number, login user, login password and Crypto key (3DES code) of the GV-AS Controller.

---

**Note:** The default values of GV-AS Controller are: IP address **192.168.0.100**; username **admin**; password **1234**; Crypto key (3DES code) **12345678**. For details see *GV-AS Controller Hardware Installation Guide*.

---

5. OPTIONAL settings in the General section:
   - **Interlock:** Enable the “interlocking” feature between two doors (Door A and Door B, or Door C and Door D). Doors that are interlocked cannot be open at the same time. One door unlock only when the other door is close.
   - **GMT:** The current time at the host computer.
   - **Enable Daylight Saving:** Enable the Daylight Saving feature. The system will automatically adjust for daylight saving time.

### 4.2.2 Step 2: Configuring a Door

1. To define the doors on the controller, click the **Door/Gate** tab. This dialog box appears.

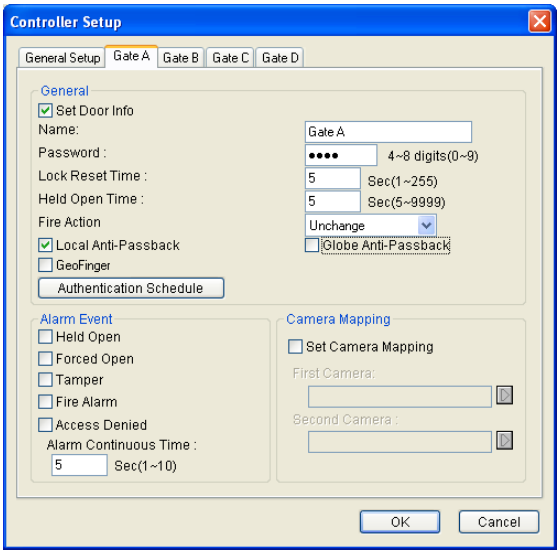



*Figure 4-3*

2. In the General section, enable **Set Door Info** to define the general parameters for the door:

   - **Name:** Give a name to the door.
   - **Password:** Give a password to the door. The default setting is 1234.
   - **Lock Reset Time:** If the door is monitored, enter the number of seconds the door can be held open. After the specified time expired, the door will automatically be locked.
   - **Held Open Time:** If the door is monitored, enter the number of seconds the door can be held open before a Door Held Open alarm is generated.
   - **Fire Action:** Set the door to be locked or unlocked when a fire alarm condition occurs.
   - **Local Anti-Passback:** To perform the Anti-Passback application, see *Chapter 6 Anti-Passback*.
   - **Global Anti-Passback:** To perform the Anti-Passback application, see *Chapter 6 Anti-Passback*.
   - **GeoFinger:** If the door is installed GeoFinger readers for fingerprint authorization, select this option.

3. To define the access mode, click the **Authentication Schedule** button. This dialog box appears.

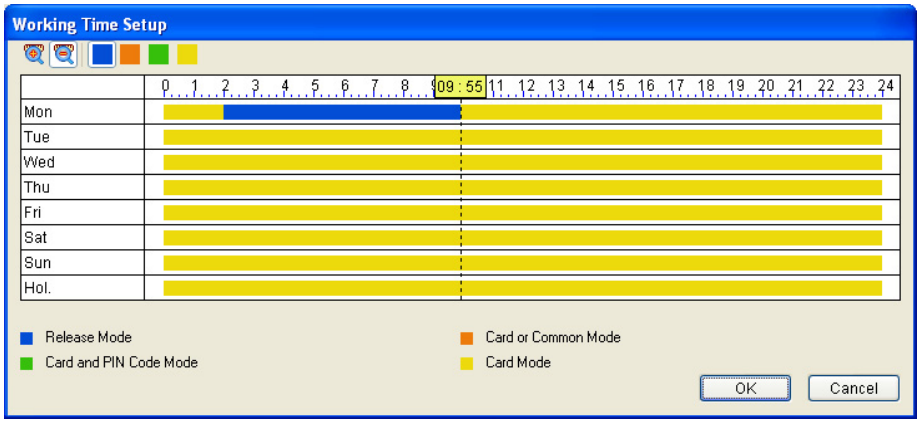



*Figure 4-4*

4. To define which kind of access mode should be applied at specific day and time, select one access mode on the toolbar and drag the mouse over the timelines. Four (4) access modes are available in the system:

   - **Card Mode:** This is the default mode. This mode only requires the user to present his card to be granted access.
   - **Release Mode:** Keep the door in an unlock status with the reader.

- **Card and PIN Code Mode:** This mode requires the user to present his card and then enter the card's PIN code on the keypad.
- **Card or Common Mode:** This mode requires the user to present his card to be granted access **OR** enter the door's password using the keypad to be granted access.

5. The settings in the Alarm Event section are OPTIONAL unless an alarm device is installed on the GV-AS Controller. Enable the desired alarm conditions that will cause the alarm to occur: **Held Open**, **Force Open**, **Tamper**, **Fire Alarm**, and **Access Denied**.
   - **Alarm Continuous Time:** Enter the number of seconds that the alarm sounds.
6. The settings in the Camera Mapping section are OPTIONAL unless a camera is installed at the secure site. For details see *Chapter 5 Video Integration*.
7. Click **OK** several times and return to the main screen. A controller folder tree will be displayed on the Device View window as example below.

   If the icon appears, it indicates the connection between the controller and GV-ASManager has been established.

   If the icon appears, it indicates the connection failed. Make sure the above connection setup is correctly configured.

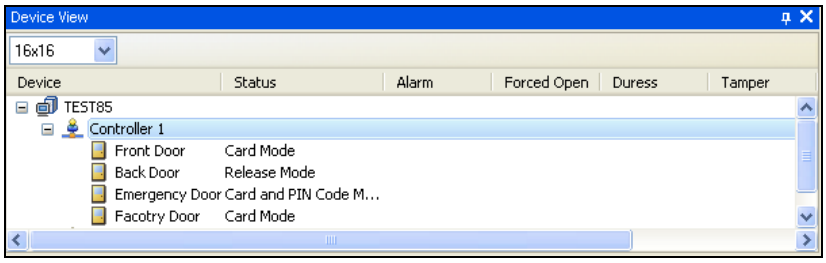



*Figure 4-5*

---

**Note:** For the disconnection messages displayed on the Status column (Figure 4-5), see *D. Controller Status* in *Appendix*.

---

## 4.3 Setting Cards

Once you have configured the controller, you may start enrolling cards. All new cards must be enrolled into the GV-ASManager before access is allowed. For the users of GV-AS200, up to 10,000 cards can be stored in the GV-ASManager; for the users of GV-AS100 and GV-AS400, up to 40,000 cards can be stored. If a card that was not enrolled is presented to the reader, the message *Access Denied: Invalid Card* will be displayed.

Depending on how many cards you need to program, you can simply add them one at a time or use the batch function to add a group of cards.

### 4.3.1 Adding a Single Card

1. To add one card, use one of these ways:
   - Present the card to the reader. The message *Access Denied: Invalid Card* is displayed. Right-click the message and select **New/Edit Card**. The New a Card dialog box appears with card number and code type entered (Figure 4-7). Then follow Step 3 to complete other settings.
   - On the menu bar, click **Personnel** and select **Cards.** This window appears.

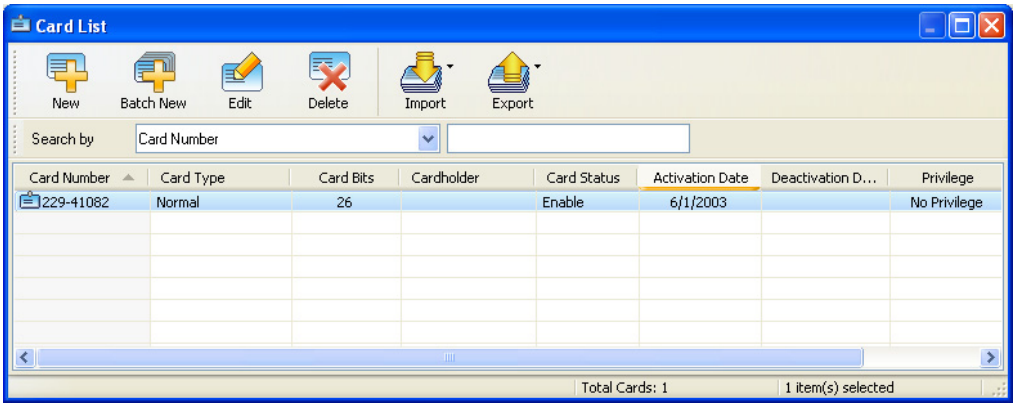



*Figure 4-6*

2. Click the **New** button on the toolbar. This dialog box appears.

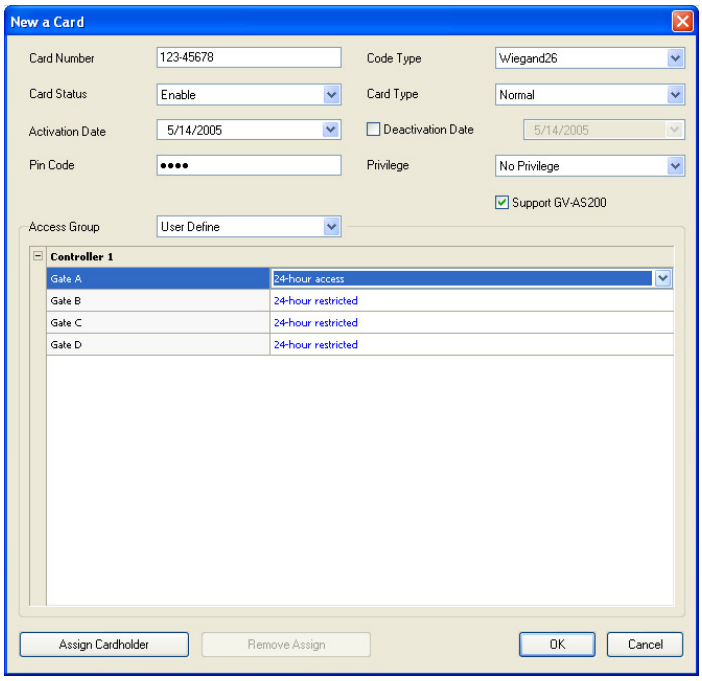



*Figure 4-7*

3. The settings are available for the card:

   - **Card Number:** Enter the card number.
   - **Code Type:** Select the code format of the card.
   - **Card Type:**
     - **Patrol:** The card is assigned to the person in charge of patrolling a location, e.g. guard. When the patrol-type card is presented to the reader, the access will be recorded but the door will NOT unlock. The feature may be set together with **Privilege** below. The user may have the privilege to stop alarm sounds and clear alarm events during patrolling.
     - **Two-person A Card:** Two-person A/B rule. The card is defined as Card A and the other Card B must be presented to unlock the two-person-rule enabled door.
     - **Two-person B Card:** Two-person A/B rule. The card is defined as Card B and the other Card A must be presented to unlock the two-person-rule enabled door.
   - **Activation/Deactivate Date:** Specify when the card is active or inactive.
   - **PIN Code:** Enter a four-digit personal code for the card. The default setting is 1234.
   - **Privilege:** Assign one of these privileges to the cardholder:
     - **Stop Alarm:** The cardholder can stop alarm sounds by presenting the card.

- **Clear Event:** The cardholder can clear alarm events by presenting the card. All alarms in the Device View window are erased. A record of these alarms is still kept in the Alarm Monitor.

- **Support GV-AS200:** If the GV-ASManager is connected to GV-AS200 and other types of GV-AS Controllers simultaneously, select this option so that the first 10,000 card data can be shared for use between GV-AS200 and another type of GV-AS Controller.
- **Access Group:** Access Groups control which personnel can access which door and at what time. For details, see *4.5 Setting Access Groups.*

  For first-time user of the GV-ASManager, the access group is not yet established. Select **User Define** for test run.
- **Controller:** The Controller column displays the associated doors. The selection for each door will be automatically brought up when one access group was entered.

  For first-time user of the GV-ASManager, select **24-hour access** for each door for test run.

4. Present the enrolled card to the reader. Once the card has been accepted, the message *Access Granted* will be displayed.

### 4.3.2 Adding a Group of Cards

Before you use the Batch function to enroll new cards, please note that the group of cards must be numbered sequentially.

1. On the menu bar, click **Personnel** and select **Cards.** The Card List dialog box appears.
2. Click the **Batch New** button on the toolbar. This dialog box appears.

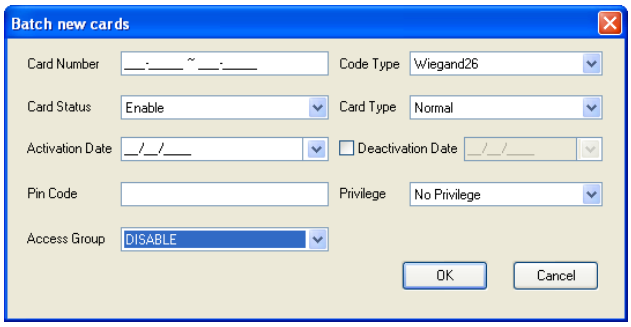



*Figure 4-8*

3. The settings in the dialog box are the same as those of adding a single card. See Step 3 in *4.3.1 Adding a Single Card*.

---

**Note:** Cards that were enrolled using the Batch function will have the same PIN. If you want to change the PINs of certain cards, you have to enter the PIN using the **Edit** function on the Card List dialog box.

---

### 4.3.3 Importing/Exporting Card Data

You can import and export card data in mdb or xls format.

**To export card data:**

1. On the Card List window (Figure 4-6), select desired cards using Ctrl + left click.
2. Click the **Export** button and select one of these options: **Export to Access** or **Export to Excel**.
3. Assign the file path, and optionally enter password to export card data.

---

**Note**: The Excel file format does not support the password protection.

---

### To import card data:

1. On the Card List window (Figure 4-6), click the **Import** button and select one of these options: **Import from Access** or **Import form Excel**.
2. Assign the file path and enter **Password** if necessary. Click **OK**. This dialog box appears.

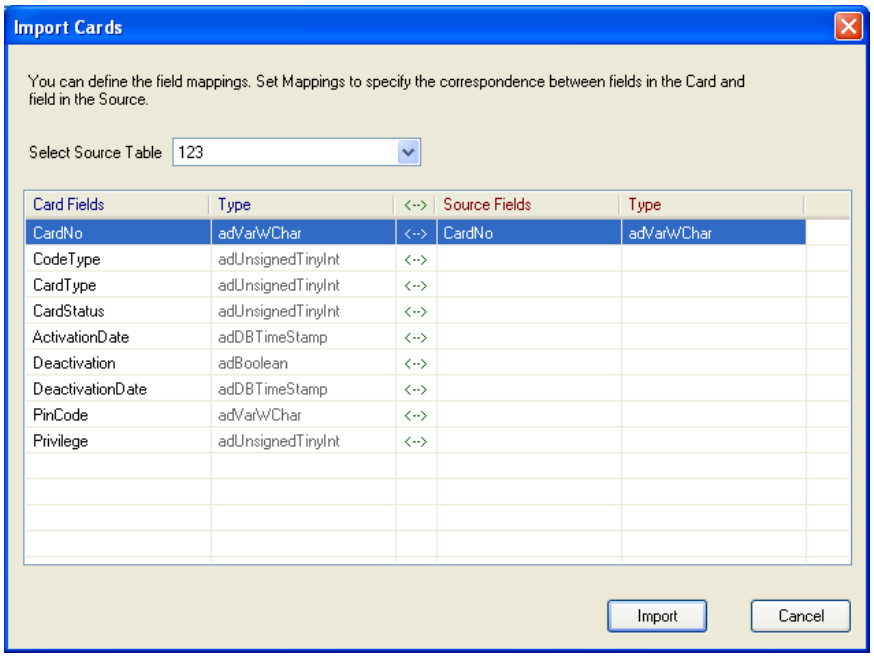



*Figure 4-9*

3. Select desired **Source Table**, and click the columns under **Source Fields** to enable the selection. Select the corresponding source items to map between Source Fields and Card Fields.
4. Click **Import** to import card data.

## 4.4 Setting Weekly Schedules

This section will help you define the daily and holiday access times. Up to 254 weekly schedules may be defined with two default weekly schedules for “deny access” and “full access”.

Before creating weekly schedules, it is helpful to map out all possible usages of weekly schedules for the site. For example: consider the variety of access hours for employees, consider requirements for janitorial personal who may need night access, consider requirements for service or repair personnel who may need all hours access, consider requirements for supervisory staff who may need extended hours access and etc.

- **Step 1 Setting Time Zones**

  Define the minutes and hours of the day when a user is granted access to a secure site. The minimum time duration is 5 minutes.

- **Step 2 Setting Weekly Schedules**

  Define the days of the week when a user is granted access to a secure site.

- **Step 3 Setting Holidays**

  Define the specific dates as holidays.

### 4.4.1 Step 1: Setting Time Zones

This section provides examples of setting the following time zones:

- Day shift – 09:00 to 19:00 hours
- Night shift – 19:00 to 9:00 hours (cross midnight)
- Supervisor – 07:00 to 24:00 hours

1. On the menu bar, click **Setup** and select **Time Zones**. This dialog box appears.

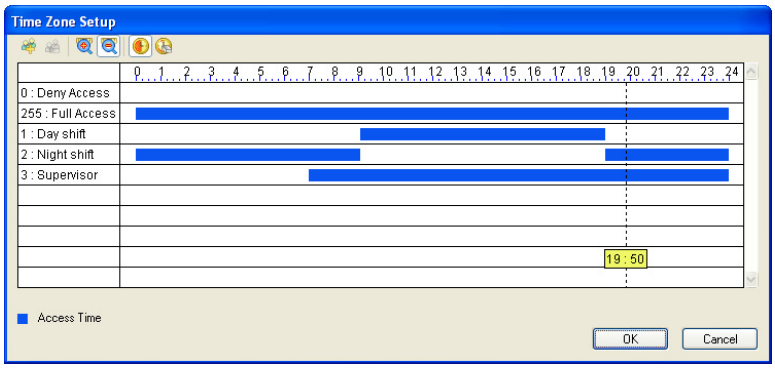



*Figure 4-10*

2. Click the **Add** button  . This dialog box appears.

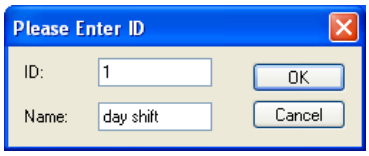



*Figure 4-11*

3. The **ID** is the number of the time zone. The system will automatically create the ID based on how many time zones have been added. Give a **Name** to the time zone you are going to define. Click **OK**.

   For example, name the Time Zone 1 as **day shift**.

4. Click the **Add Access Time** button  . Then drag the mouse on the timeline to define a period of access time.

   For example, the time of day shift is **from 09:00 to 19:00**.

5. To create the second time zone, click the **Add** button and name it as **night shift**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 19:00 to 24:00** and **from 00:00 to 09:00**.

6. To create the third time zone, click the **Add** button and name it as **Supervisor**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 07:00 to 24:00**.

7. Click **OK**. The three time zones have been defined.

### 4.4.2 Step 2: Setting Weekly Schedules

This section provides examples of setting the following weekly schedules:

- Schedule-Day shift – Monday through Friday, 09:00 to 19:00 hours
- Schedule-Night shift – Monday through Friday, 19:00 to 9:00 hours
- Schedule-Supervisor – Monday through Sunday and Holidays, 07:00 to 24:00 hours

1. On the menu bar, click **Setup** and select **Weekly Schedules**. This dialog box appears.

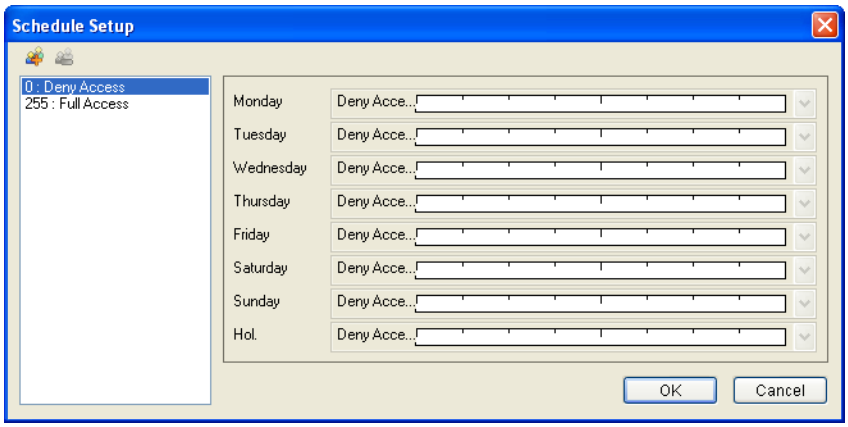



*Figure 4-12*

2. Click the **Add** button. This dialog box appears.

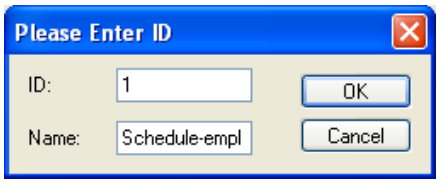



*Figure 4-13*

3. The **ID** is the number of the weekly schedule. The system will automatically create the ID based on how many time schedules have been added. Give a **Name** to the weekly schedule you are going to define. Click **OK**.

   For example, name the Weekly Schedule 1 as **Schedule-Day shift**.

4. From the drop-down lists of **Monday** to **Friday**, select the **Day shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.

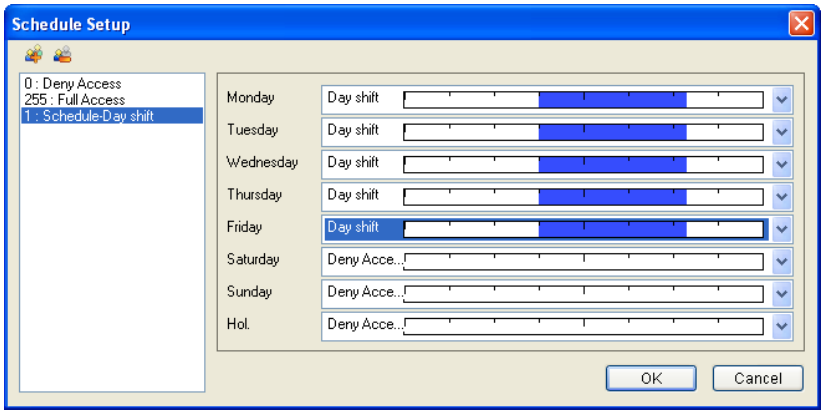



*Figure 4-14*

5. To create the second time schedule, click the **Add** button and name it as **Schedule-Night shift**. From the drop-down list of **Monday** to **Friday**, select the **Night shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.

6. To create the third time schedule, click the **Add** button and name it as **Schedule-Supervisor**. From the drop-down lists of **Monday** to **Hol**, select **Supervisor** time zone we have created.

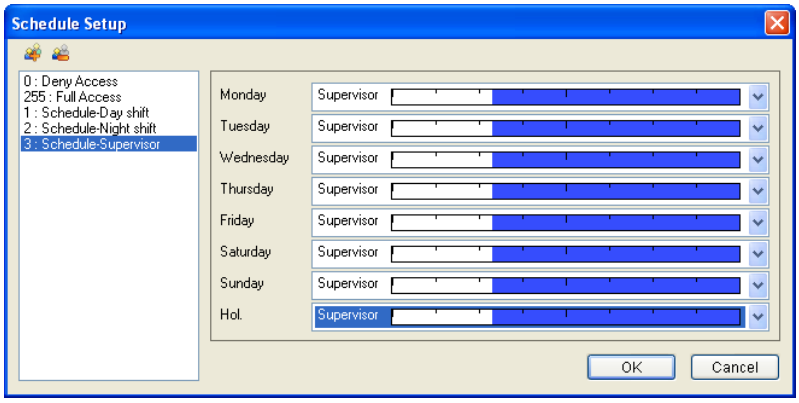



*Figure 4-15*

7. Click **OK.** The three weekly schedules have been defined.

### 4.4.3 Step 3: Setting Holidays

To designate the specific dates as holidays on the system:

1. On the menu bar, click **Setup** and select **Holidays**. This dialog box appears.

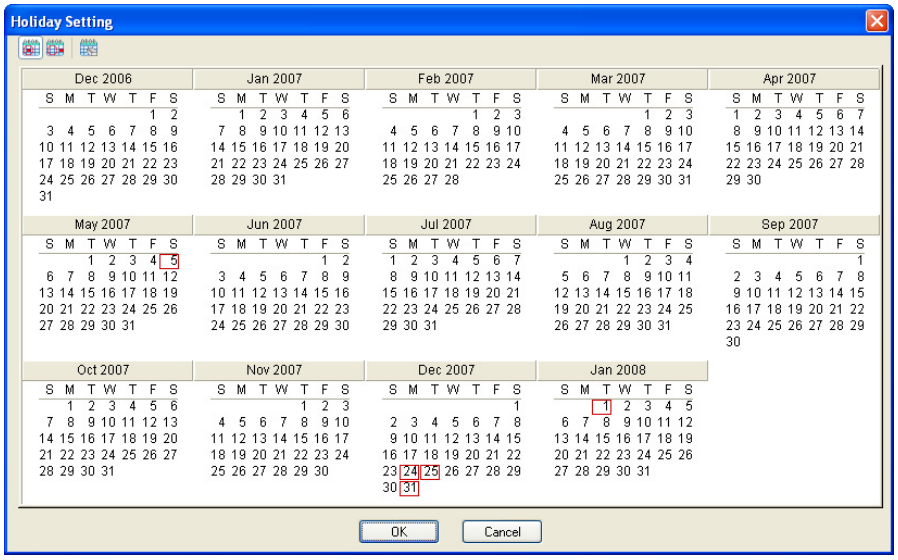



*Figure 4-16*

2. Click the **Holiday** icon and click the specific dates as holidays. For example,
   - Dec 24, 2007 – Christmas Eve
   - Dec 25, 2007 – Christmas Day
   - Dec 31, 2007 – New Year's Eve
   - Jan 01, 2008 – New Year's Day
3. To delete the holiday, click the **Non Holiday** icon and click the date you want to delete.

---

**Note:** Holiday dates can cross over to the following year, and certain holiday dates change from year-to-year. Administrators should review and update the holiday setting prior to the beginning of a new year to ensure proper holiday coverage.

---

## 4.5 Setting Access Groups

Access groups restrict which personnel can access which door, and at what time and day. To be granted access to a secure door, a user must meet the criteria of the access group. The user must be at a door that accepts the members of that access group, and it must be during a weekly schedule that allows that user access.

This section uses an example to describe how to create an access group and assign the criteria of the access group to a card. In this example, the FAE staff of day shift needs access to the front and back doors during the day shift time.

1. On the menu bar, click **Setup** and select **Access Groups**. This dialog box appears.

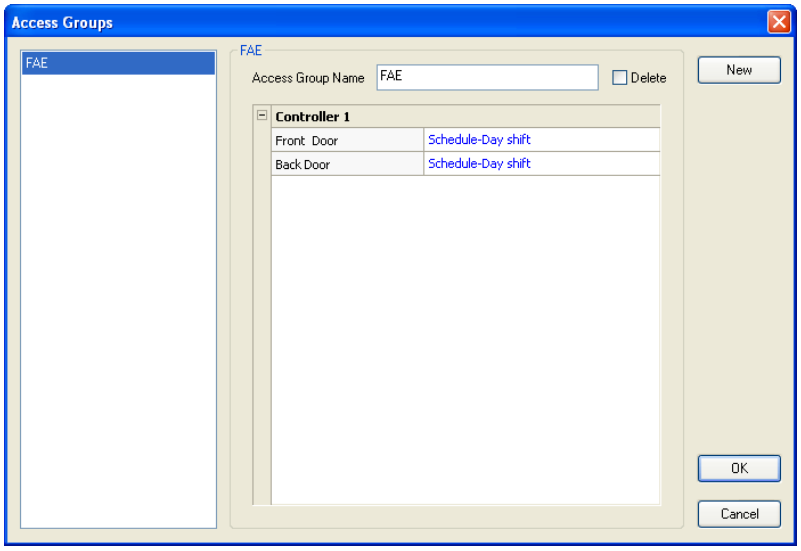



*Figure 4-17*

2. Click the **New** button, and give a **Name** to the new access group.

   For example, name the access group as **FAE**.

3. To define door access for the access group, click the drop-down list of each door and select one of pre-defined Weekly Schedules.

   For example, click each blue field of **Front Door** and **Back Door**, and then select **Schedule-Day shift**.

4. Click **OK**. The access group for the FAE staff has been created.

5. To assign the criteria of the access group to a single card, click **Personnel** on the menu bar and select **Cards**. The Card List dialog box appears.

6. Double-click one listed card. This dialog box appears.

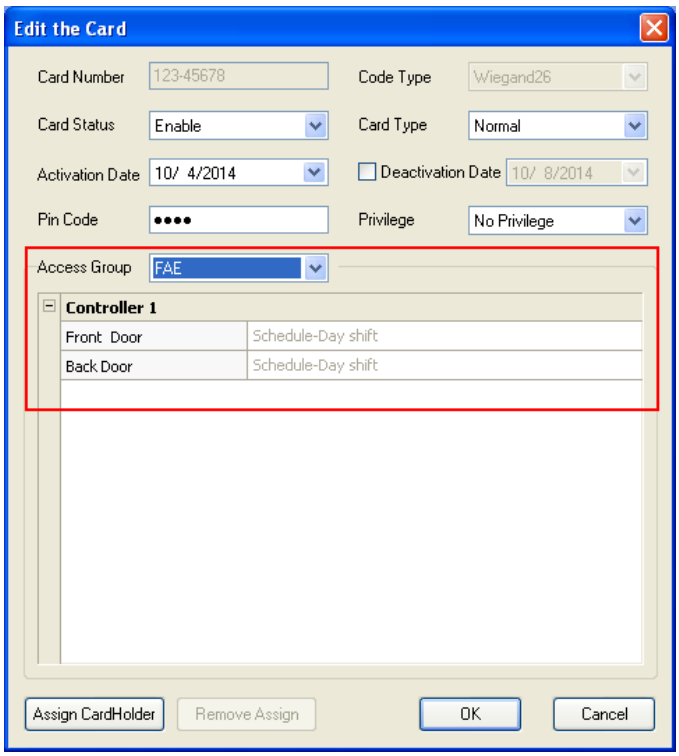



*Figure 4-18*

7. From the **Access Group** drop-down list, select one pre-defined access group, e.g. **FAE**. The assigned Weekly Schedule will be displayed on the associated door's field.

## 4.6 Setting Cardholders

This section describes how to create a database of cardholder information, and assign cards to cardholders.

### 4.6.1 Adding a Cardholder

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Click the **New** button on the toolbar. This dialog box appears.

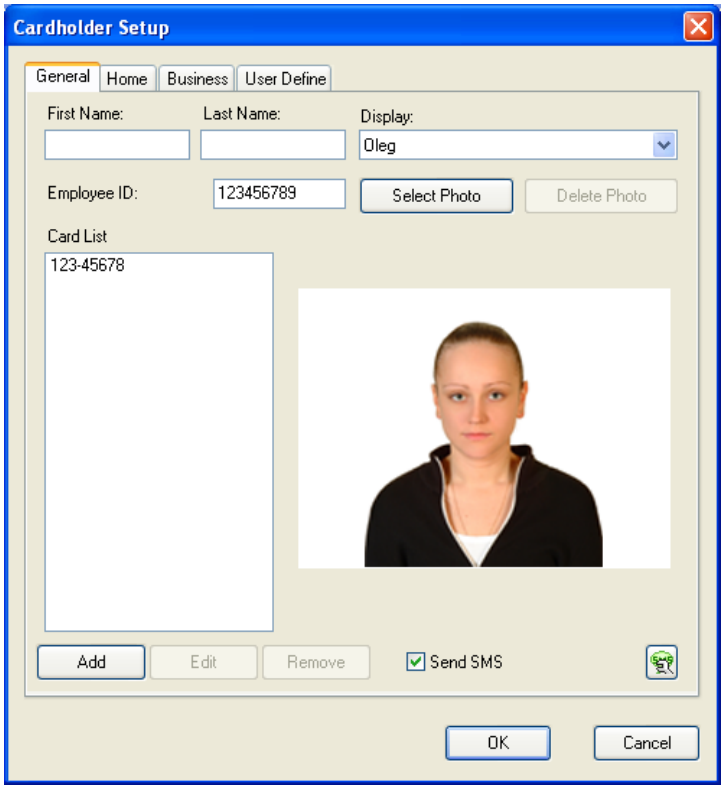



*Figure 4-19*

3. Enter a name under **Display** that is stored as minimum. Other information of the cardholder such as Employee ID, Photo, Home information and Company information are optional entries.

### 4.6.2 Assigning a Card to a Cardholder

There are two methods to assign a card to a cardholder.

---

**Note:** At this step we assume that you have followed the instructions in *4.3 Setting Cards* to complete your card enrollment.

---

1. On the Cardholder Setup dialog box (Figure 4-19), click **Add** and double-click one listed card to assign the card to the cardholder.
2. On the Edit Card dialog box (Figure 4-18), click **Assign Cardholder** and double-click one listed cardholder to assign the cardholder to that card.

### 4.6.3 Sending SMS Alerts

If you want to send SMS alerts whenever the card(s) assigned to the cardholder is presented to the reader, select **Send SMS** in the Cardholder Setup dialog box.

Before sending the SMS, see *7.2.1 Setting SMS Server* to configure the SMS server. For how to set up SMS alerts, refer to the same settings “Send SMS Alert” at Step 3 in *7.2.3 Setting Notification*.

### 4.6.4 Customizing a Data Field

You can customize data fields for cardholders. Up to ten data fields can be created for user data entry.

When a custom data field is created, the field label will be displayed in the User Define tab on the Cardholder Setup dialog box. The actual personal data for each user is entered in the User Define tab.

#### To customize a data field:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Click the **User Define Fields Setting** button on the toolbar. The User Define Fields Setting dialog box appears.

3. Select one **User Define** field, and enter the text to be displayed as the field label. In this example, a Car License Plate field was created.

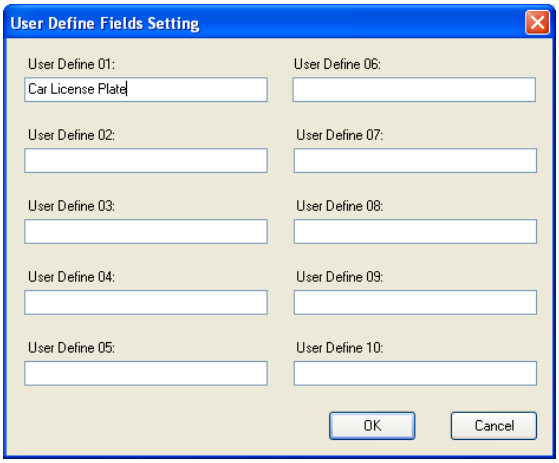



*Figure 4-20*

## To enter personal data:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Double-click one listed user to whom personal data should be entered. The Cardholder Setup dialog box appears.
3. Click the **User Define** tab. The custom data field you have created now is displayed.
4. Click in the custom data field and enter the appropriate information. In this example, a number is entered in the created Car License Plate field:

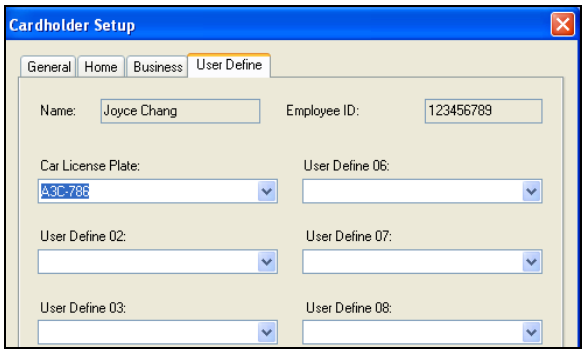



*Figure 4-21*

### 4.6.5 Importing/Exporting Cardholder Data

From the Cardholder List window, you can import and export cardholder data in mdb or xls format. For this function, please refer to *4.3.3 Importing/Exporting Card Data.*

# Chapter 5 Video Integration

GeoVision IP devices and certain third-party IP cameras can be connected to the GV-ASManager through the network. Live video can then be accessed for monitoring and surveillance purposes.

The GV-ASManager provides the following video features:

- Live view
- Video playback
- Monitor up to 16 cameras at one time

---

**Note:**

1. GeoVision IP devices include GV-System, GV-NVR, GV-Video Server, GV-Compact DVR and GV-IP Camera. For compatible third-party IP cameras, see Appendix A.
2. The GV-ASManager only supports GV-System of version 8.120 or later.

---

**Hint:** In the following sections the term “DVR” refers to GV-System and GV-NVR, the term “Video Server” refers to GV-Video Server and the term “Compact DVR” refers to GV-Compact DVR.

---

## 5.1 Mapping Cameras

If you want to map a camera from the DVR to a door, the DVR must be enabled for video access ahead:

- Enable **Control Center Server** (CCS)

To map cameras to a door:

1. On the menu bar, click **Setup** and select **Device**. The Controller List dialog box appears.
2. Double-click one listed controller. The Controller Setup dialog box appears.

3. Click one **Door** tab. This dialog box appears.

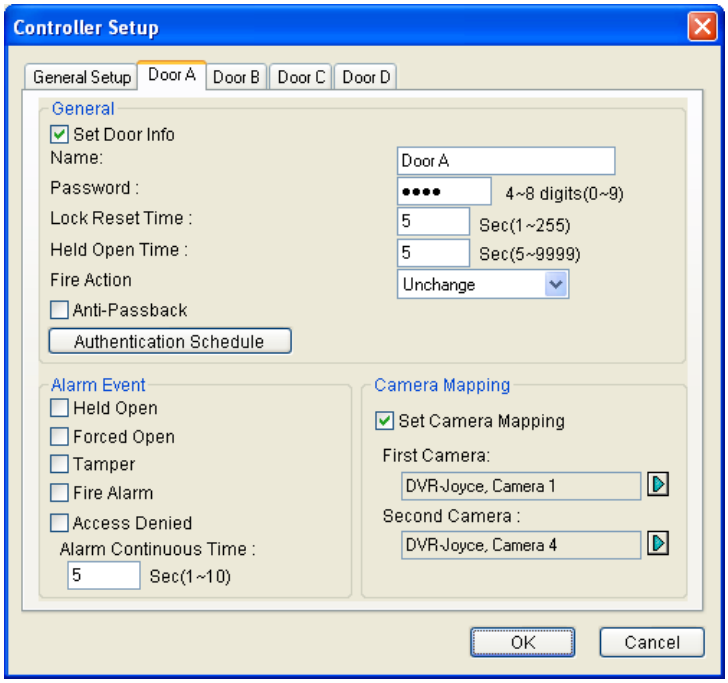



*Figure 5-1*

4. In the Camera Mapping section, select **Set Camera Mapping** and click the first **Arrow** button. This dialog box appears.

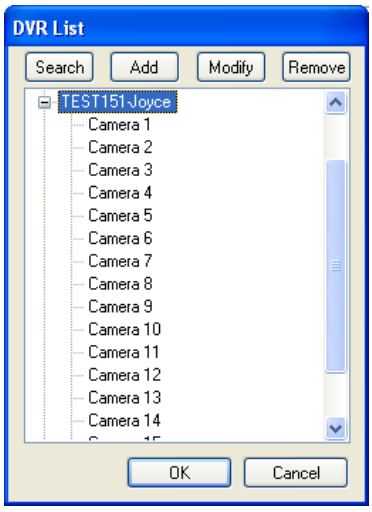



*Figure 5-2*

5. To connect one IP device to the GV-ASManager, use one of these ways:

   - Click **Add**, select the type of the IP device, and enter its IP address and login information.
   - Click **Search** to detect all GeoVision IP devices on the same LAN. After the found IP device is added, you must click the **Modify** button to enter its login ID and password.

6. Expand the Host folder listed in the DVR List dialog box (Figure 5-2), select one camera and click **OK**. The mapped **Host Name** and **Camera** are displayed on the Controller Setup dialog box.
7. To map the second camera to the door, click the second **Arrow** button, and follow Steps 5 and 6 to add another camera.
8. Click **OK** and return to the main screen.
9. Click the specific door on the Device View window. The associated live view is displayed on the Live Video window.

---

**Tip:** You can modify the host or camera name in the DVR List dialog box (Figure 5-2) by clicking the listed name directly.

---

## 5.2 Accessing a Live View

After mapping cameras to doors, use one of the following methods to access a live view on the Live Video window:

- On the Device View window, click the desired door. Its associated live view will appear.
- On the Camera List window, click the desired camera. Its associated live view will appear.
- On the Alarm Monitor and Access Monitor windows, click the desired event. Its associated live view will appear.

To access live views from multiple IP devices, see *5.4 The Multiview Window* below.

### 5.2.1 Live Video Window

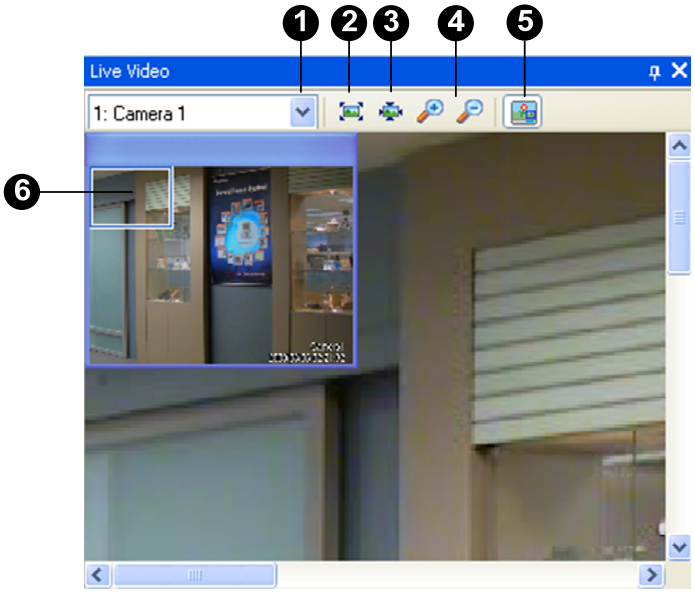



*Figure 5-3*

The controls on the Live Video window:

| No. | Name | Function |
|---|---|---|
| 1 | Camera List | Switches between two cameras when you have mapped two cameras to the selected door. |
| 2 | Best Fit | Rescales the image to fit any resized window. |
| 3 | Actual Size | Displays the image in its original size. |
| 4 | Zoom | Zooms in or out the image. |
| 5 | Thumbnail | Displays a thumbnail view (No. 6). When the image size is larger than the Live Video window, drag the box in the thumbnail view to have a close look at the image. |
| 6 | Thumbnail View | See the description in No. 5. |

**Note:** For Windows 2000, the camera name displayed in the camera list of the Live Video window will not be updated automatically after the camera name is modified. You need to select the corresponding camera on the Camera List window (No. 11, Figure 3-1) to update the camera name manually.

## 5.3 Accessing a Video Image

You can access the video image captured after the access and alarm triggered event.

- On the Access Monitor or Alarm Monitor window, double-click the desired event to display the image. Or, right-click the desired event and select **Show Image** to display the image. Notice if there is no image retrievable, the option will be grayed out.

## 5.4 The MultiView Window

The MuliView window provides a quick view of up to sixteen preset cameras on one screen. These cameras can be a mix of cameras from several IP devices.

To open and use MulitView:

1. On the menu bar, click **View** and select **MultiView**. The MultiView window appears, similar to Figure 5-4.
2. Drag the desired camera from the Camera List window, and drop it to the required frame on MultiView.

The video generated by the camera appears in this frame. If a different camera view already exits in this frame, the new video takes its place.


*Figure 5-4*

The controls on the MultiView window:

| No. | Name | Function |
|---|---|---|
| 1 | Frame | The frame displays live video from the assigned camera. The camera number and name, controller ID and name will be displayed in the upper left corner. |
| 2 | 3D | Click this option to have a dynamic 3D live view. In the 3D live view:<br>• Double-click one camera view to switch between 3D mode and thumbnails. Then right-click the 3D image to have different 3D effects.<br>• Double-click one camera view in thumbnails to change different divisions (4, 9 and 16 divisions). |
| 3 | Camera List | Select the desired camera. The selected camera will be displayed with mouse focus. For Windows 2000, the list is not available. |
| 4 | Previous / Next Page | Go to the previous or next page of camera views. |
| 5 | Matrix View | Select an existing Matrix View (a group of views) from the drop-down list. For details, see *5.4.1 Adding a Matrix View*. |
| 6 | Add Matrix | Add a Matrix View. |
| 7 | Delete Matrix | Delete a Matrix View. |
| 8 | Resolution | Select the image resolution. Double-click one camera view to rescale the image to fit the MultiView window or restore to its set resolution. |

**Note:** It is possible to drag the MultiView window out of the main screen and even drag the window to place at the second computer monitor.

### 5.4.1 Adding a Matrix View

A Matrix View, or a group of views, is a programmed arrangement of frames in the MultiView window that can present up to sixteen different camera views. Multiple Matrix Views can be added as required.

1. In the Matrix View drop-down list (No. 5, Figure 5-4), enter a name for the Matrix View.
2. Click the **Add Matrix** button. The Matrix View name is created.
3. Drag the desired camera from the Camera List window to an available frame in the window. The video associated with the camera is displayed in the frame.
4. You can repeat Steps 1-3 to add more than one Matrix View. And use the drop-down list to change to a different Matrix View.

## 5.5 Retrieving Recorded Video

Recorded video can be reviewed by retrieving the video from the DVR (GV-System / GV-NVR) and playing it back. Before you can review video recorded on the DVR, the following function must be enabled to allow remote access:

- DVR: Enable **Remote ViewLog Service** on Control Center Server

To play back video:

- On the Access Monitor or Alarm Monitor window, click the desired event. If recorded video exits, the Playback window will be enabled. Click the **Play** button to play the video clip.

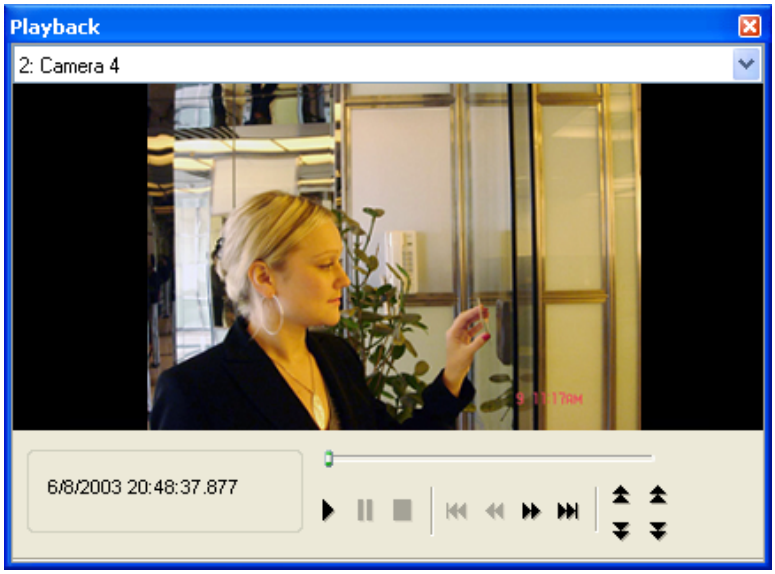
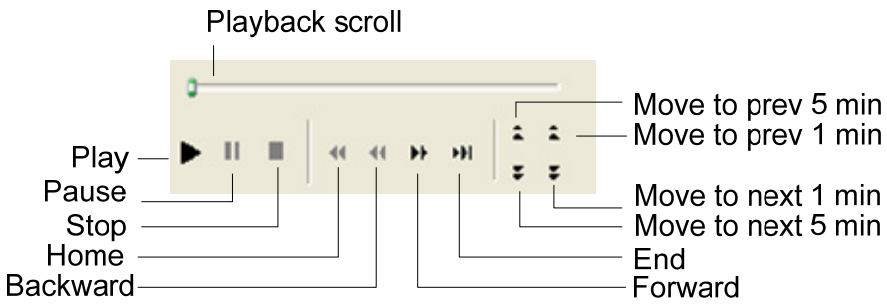



*Figure 5-5*



Right-click the window to have the following features:

| | |
|---|---|
| **Play Mode** | Includes these options:<br>• **Frame by Frame:** Plays back video frame by frame.<br>• **Real Time:** Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback.<br>• **Auto Play Next 5 Minutes:** Plays back video up to 5 minutes.<br>• **Audio:** Turns on or off the video sound. |
| **Render** | Includes these options:<br>• **Deinterlace:** Converts the interlaced video into non-interlaced video.<br>• **Scaling:** Smoothens mosaic squares when enlarging a playback video<br>• **Deblocking:** Removes the block-like artifacts from low-quality and highly compressed video.<br>• **Defog:** Enhances image visibility.<br>• **Stabilizer:** Reduces camera shake.<br>• **Text overlay's camera name and time:** Overlays camera name and time onto the video.<br>• **Text overlay's POS/GV-Wiegand:** Overlays POS or GV-Wiegand Capture data onto the video.<br>• **Full Screen:** Switches to the full screen view. |
| **Tools** | • **Snapshot:** Saves a video image.<br>• **Save as AVI:** Saves a video as avi format.<br>• **Download:** Downloads the video clip from a GeoVision IP device to the local computer. |

**Note:** For Windows 2000, the camera name displayed in the Camera List of the Playback window will not be updated automatically once the camera name is modified. You need to select the corresponding camera on the Camera List window (No. 11, Figure 3-1) to update the camera name manually.

# Chapter 6 Anti-Passback

The Anti-Passback is used to ensure one-card and one-way access into and then out of a controlled area. This function prevents card holders from passing their cards back to a second person to gain entry into the same controlled area. Depending on the number of controllers and communication link, there are three types of Anti-Passback operations: **Anti-Passback**, **Local Anti-Passback** and **Global Anti-Passback**.

Anti-Passback is performed only on one controller, while Local Anti-Passback and Global Anti-Passback can be performed on multiple controllers. Anti-Passback is performed through either RS-485 or TCP/IP connection, while Local Anti-Passback and Global Anti-Passback are performed only through TCP/IP connection. The following table lists the supported operations among GV-AS Controllers.

| Model | Anti-Passback | Local Anti-Passback | Global Anti-Passback |
|---|---|---|---|
| GV-AS100 | Yes | Yes (GV-ASBox required) | Yes (GV-ASBox required) |
| GV-AS200 | Yes | Yes (Firmware 1.1 or later) | No |
| GV-AS400 | Yes | Yes | Yes |

**Note:** For GV-AS200 users, the Local Anti-Passback function is only available on GV-AS200 firmware 1.1 or later.

## 6.1 Anti-Passback

Anti-Passback is used on **one controller only**. For this application, select **Local Anti-Passback** at the **Gate** tab of the Controller Setup dialog box (Figure 4-3).

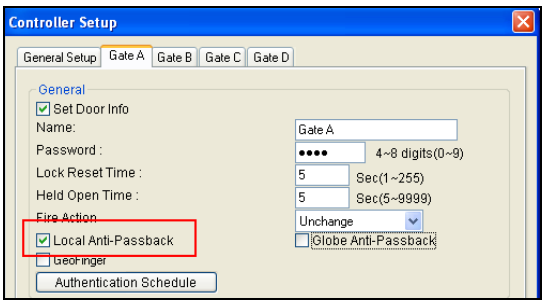



*Figure 6-1*

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

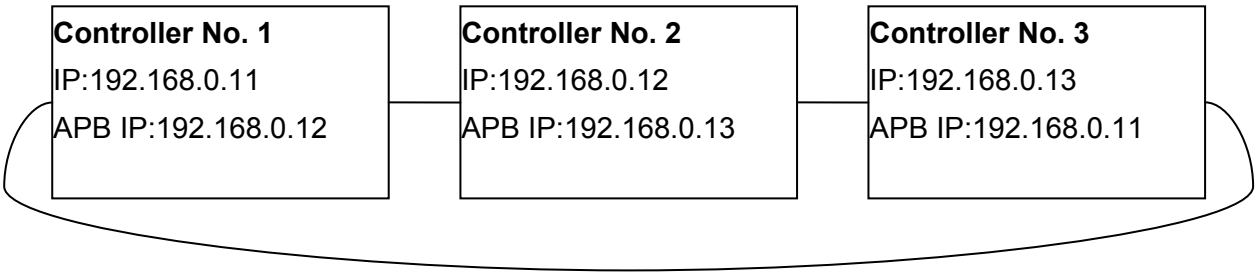
## 6.2 Local Anti-Passback

Local Anti-Passback is used on **multiple controllers which are associated with network connections**. Before you start, the following conditions must be true:

- The communication mode between GV-ASManager and GV-AS Controller is Ethernet.
- For the users of GV-AS200, the firmware is V1.10 or later.
- LAN environment is applied.

Here we use three **GV-AS200 Controllers** as example to explain how to combine three controllers together to operate the Anti-Passback (APB) function. Since Anti-Passback is performed in a network connection, every controller has a unique IP address. When three controllers are connected for Anti-Passback, an APB IP address is then applied for interaction.

For example, Controller No. 1, No. 2 and No. 3 are combined in sequence, as illustrated below. APB IP is the IP address of the associated controller.
IP of Controller No. 1 is 192.168.0.11; APB IP of Controller No. 1 is IP of Controller No. 2.
IP of Controller No. 2 is 192.168.0.12; APB IP of Controller No. 2 is IP of Controller No. 3.
IP of Controller No. 3 is 192.168.0.13; APB IP of Controller No. 3 is IP of Controller No.1.



To configure Anti-Passback for the three GV-AS200 Controllers:

1. Access the **AS200 Setting** page of the Controller No. 1 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 2, e.g. 192.168.0.12.

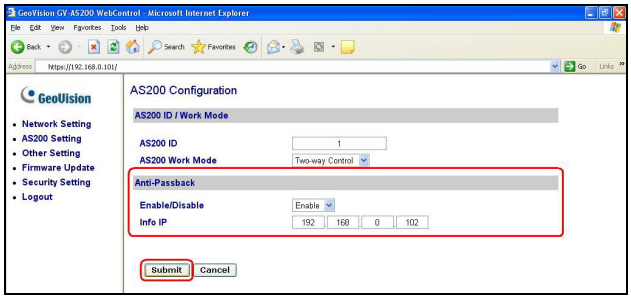



*Figure 6-2*

2. Access the **AS200 Setting** page of the Controller No. 2 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 3, e.g. 192.168.0.13.
3. Access the **AS200 Setting** page of the Controller No. 3 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 1, e.g. 192.168.0.11.
4. On the ASManager, select **Local Anti-Passback** (Figure 6-1) to start the function.

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

## 6.3 Global Anti-Passback

Global Anti-Passback can not only prevent the use of a card to gain successive entries, but track the card holder around the site. This application is only available for **GV-AS100** and **GV-AS400**.

The diagram below shows a typical site controlled by access control. The following sections will guide you through the steps you would need to go through to configure this site for Global Anti-Passback.

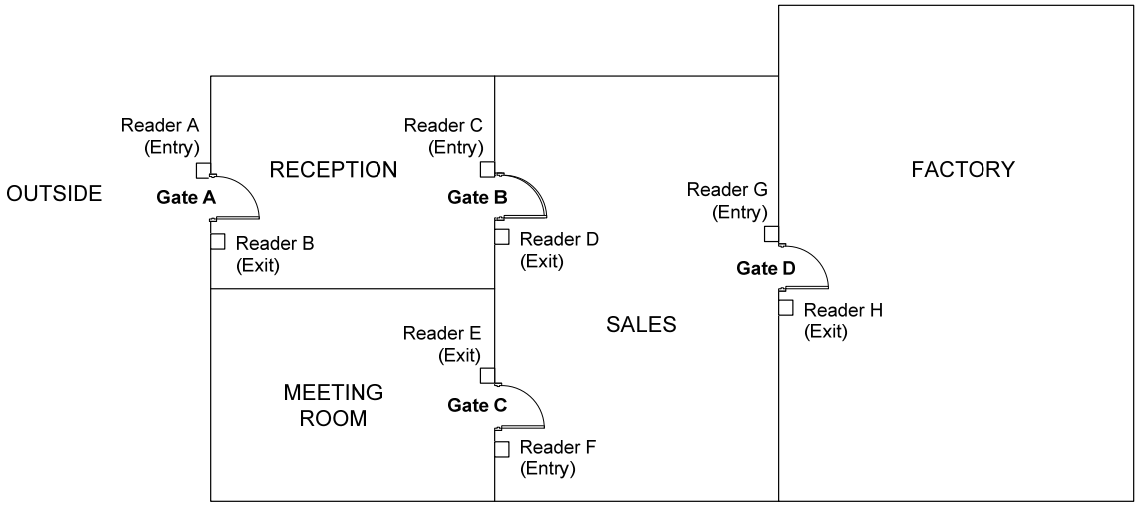



*Figure 6-3*

### 6.3.1 Step 1: Enabling Global Anti-Passback

Select **Global Anti-Passback** at each **Gate** tab of the Controller Setup dialog box (Figure 4-3).

### 6.3.2 Step 2: Configuring Areas

This step is to define the Entry and Exit areas for each door/gate and name the areas properly.

- On the menu bar, click **Setup** and select **Areas**. This dialog box appears.

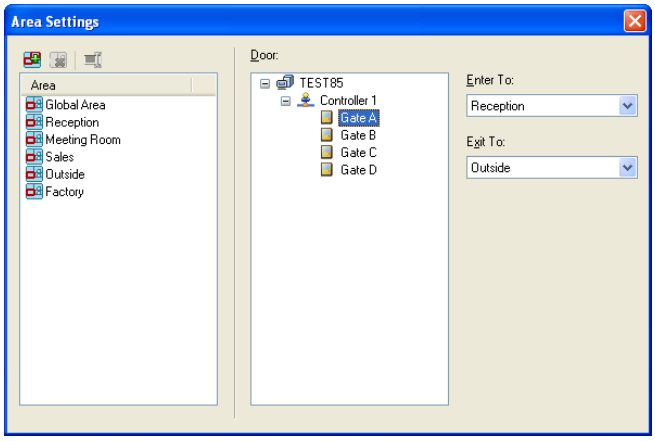



*Figure 6-4*

**Enter to** is the area where you enter by accessing the Entry reader. **Exit to** is the area where you exit to by accessing the Exit reader. In this case, we set up like this:
Gate A: **Enter to** Reception; **Exit to** Outside
Gate B: **Enter to** Sales; **Exit to** Reception
Gate C: **Enter to** Meeting Room; **Exit to** Sales
Gate D: **Enter to** Factory; **Exit to** Sales

### 6.3.3 Step 3: Configuring Readers

This step is to define the Entry and Exit readers for each door/gate. The reader definition tells the GV-ASManager which reader controls the access across the area boundaries.

When card holders access the unauthorized readers, the message **Access Denied: APB (Wrong Area)** will be displayed and the door will remain locked. When card holders access the same reader successively, the message **Access Denied: APB (Double Entry)** will be displayed and the door will remain locked.

To define readers, you can use GV-ASKeypad or the Web interface of the GV-AS Controller. Here we use the GV-AS400 Web interface as example to define Wiegand readers. For this case, Wiegand reader A (Entry) goes from Outside to Reception, Wiegand reader B (Exit) goes from Reception to Outside and etc.

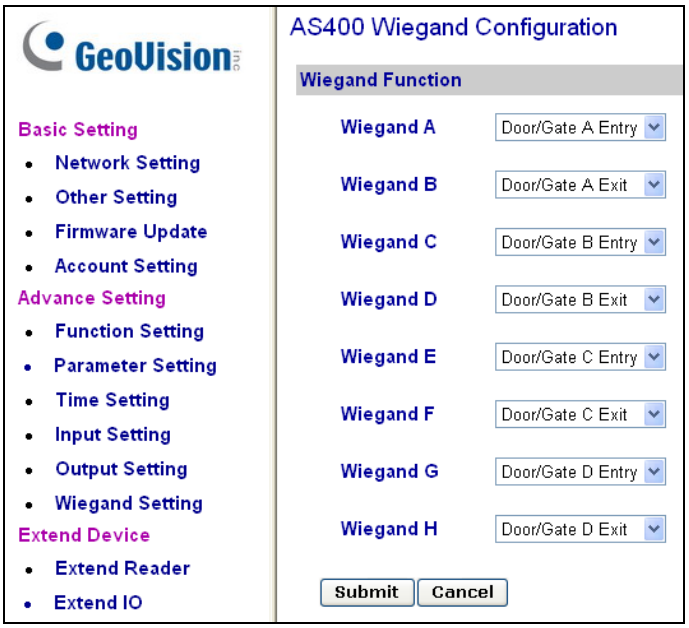



*Figure 6-5*

### 6.3.4 Step 4: Configuring Door Contacts

This step is to define the door contact sensor for each door/gate. When the door contact sensor is triggered and the door is unlocked, the GV-ASManager can tell where a card holder is based on your area definition at Step 1.

To define door contact sensors, you need to use the Web interface of GV-AS Controller. In this example of GV-AS400 Web interface, Input 01 is used as Door Contact of Door A, Input 02 is used as Door Contact of Door B and etc.

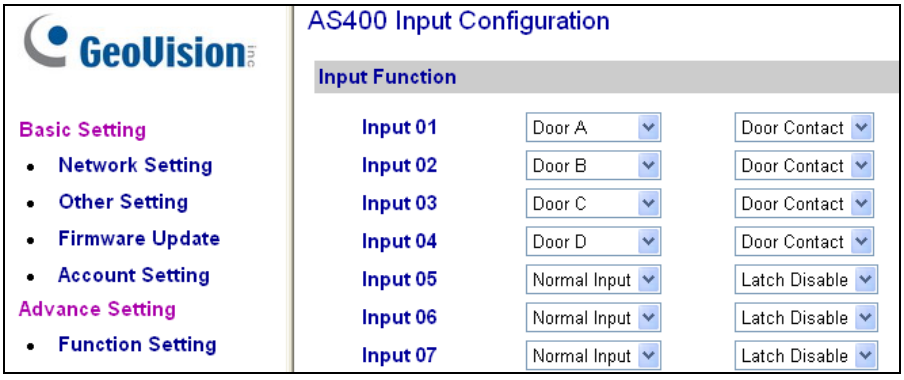



*Figure 6-6*

### 6.3.5 Step 5: Locating Card Holders

To locate a card holder, select **Monitoring** on the menu bar and select **New Locate Person**. When the Exit or Entry reader is triggered, the GV-ASManger can tell if card holders follow Anti-Passback rules and then grand or deny the access. When the door contact sensor is triggered, the GV-ASManager can tell the location where the card holder is now.

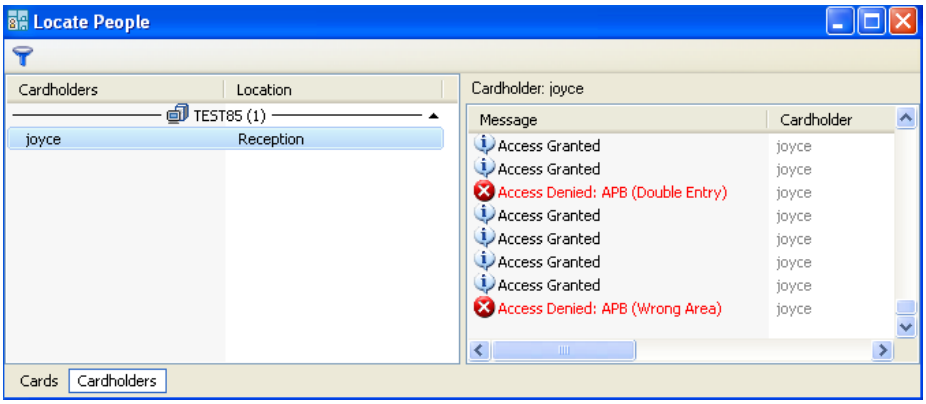



*Figure 6-7*

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

# Chapter 7 Other Functions

## 7.1 System User Setup

A system user is a person using the GV-ASManager to monitor door controllers, enroll cardholders or program the system. Using this function, the system supervisor can create new system users with different access rights. Up to 1,000 user accounts can be created.

### 7.1.1 Adding a New User

1. On the menu bar, click **Tools** and select **Accounts**. This dialog box appears

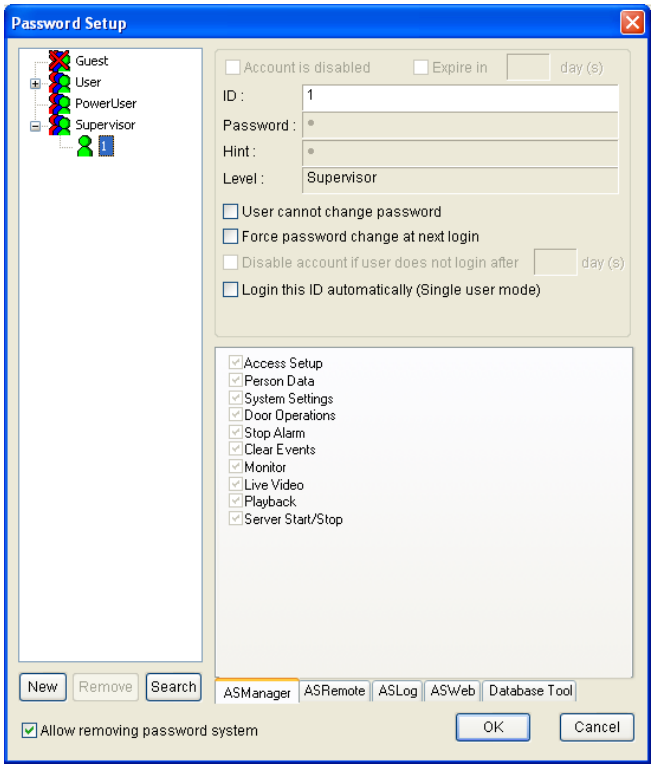



*Figure 7-1*

2. Click **New** at the lower left corner. This dialog box appears.

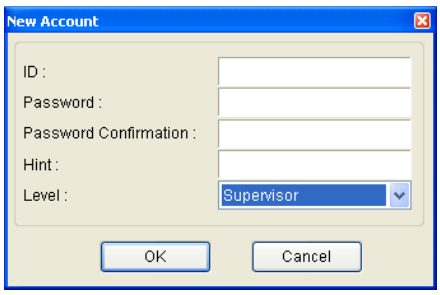



*Figure 7-2*

3. Enter the user's **ID** and **Password**. Re-enter the same password in the Password Confirmation field.
4. Give a **Hint** (optional) that would remind you of the password.
5. Select the user's authorization level: **Supervisor**, **PowerUser** or **User**. By default, users belonging to the Supervisor level have full rights and permissions to system settings. PowerUsers have the same rights and permissions as Supervisors, except that they cannot edit user information and delete the password system (described later). Users belonging to the User level are restricted to all system settings, and have only limited access to certain functions.
6. Click **OK** to add the user.
7. Click the tab **ASManager**, **ASRemote**, **ASLog**, **ASWeb** or **Database Tool** in the lower part of the window. Check and uncheck the functions to which the system user should be authorized.
8. Other settings are available:
   - **Expire in xx day(s):** The account will expire and be disabled automatically after a set number of days. The number you set will count down automatically. Specify the number between 1 and 9999.
   - **User cannot change password:** The user is not allowed to change the set password.
   - **Force Password change at next login:** The user must change the password when logging in first time.
   - **Disable account if user does not login after xx day (s):** When the user does not log in the system after a set number of days, its account will be disabled automatically.
   - **Allow removing password System:** This option lets the user remove the ID and password database from the system. To do this, select this option (only Supervisor can enable the option), and then find **PassUnInStall** in the system folder. Click the program and a message prompts you for confirmation. Click **Yes** to remove the entire ID and password from the system.

---

**Note:** If the **Allow Removing Password System** option is not checked, the loss of passwords will require the reinstallation of Windows and the reset of passwords.

---

### 7.1.2 Editing an Exiting User

Only supervisors are allowed to edit the information of a system user.

1. Select a user from the user list to display its properties. Or, right-click on any of the user levels (User, PowerUser, Supervisor), and then select **Find Specific Account** for a quick search. A valid password is required to edit a supervisor.
2. Edit the properties as required. Check the **Account Is Disabled** option if you wish to disable this user.

### 7.1.2 Changing Password at Login

1. When you log in the system, click the **Change Password** button in the Login dialog box. The Change Password dialog box appears.

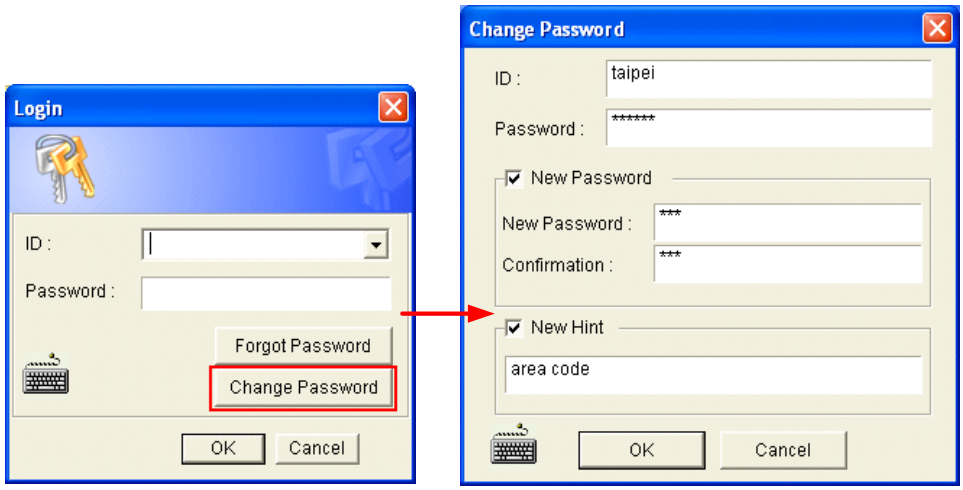



*Figure 7-3*

2. Type the new password information, and click **OK** to save the changes.

---

**Note:** If the user is not given the right to change password, the message *Change Password/Hint False* will be displayed.

---

## 7.2 Notification Setup

When alarm conditions occur the system can automatically send SMS alerts and e-mail alerts to one or multiple recipients, as well as activating computer alarm.

### 7.2.1 Setting SMS Server

Before you can send out SMS alerts, you should configure the SMS server.

1. On the menu bar, click **Tools** and select **SMS Server Settings**. This dialog box appears.

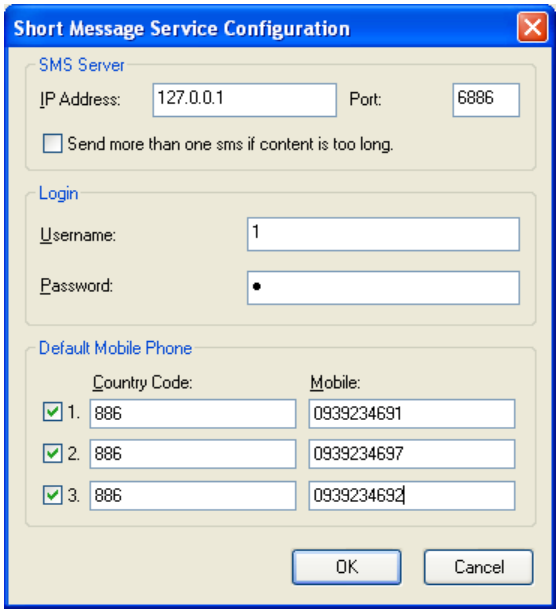



*Figure 7-4*

2. Type the IP address of the SMS server, its login username and password. Then assign up to three mobile numbers, including country code, which SMS alerts should be sent to. Click **OK**.
3. To enable the SMS connection, click **Tools** on the menu bar and select **Connect to SMS Server**.

---

**Note:** For ASCII encoding (English language), SMS text messages are limited to 160 characters; for Unicode encoding (other languages), SMS text messages are limited to 70 characters. If you want to send longer text messages, select **Send more than one sms if content is too long.** The long messages will be split up to 9 segments and go out as multiple SMS messages.

---

### 7.2.2 Setting E-Mail Server

Before you can send out e-mail alerts, you should configure the e-mail server.

1. On the menu bar, click **Tools** and select **Email Server Settings**. This dialog box appears.

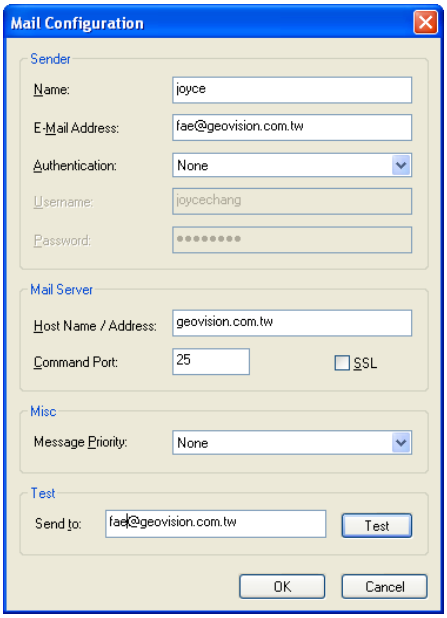



*Figure 7-5*

2. Set up the following options:

   - **Name:** Type the sender's name.
   - **E-Mail Address:** Type the sender's e-mail address.
   - **Authentication:** If your mail server requires authentication for sending e-mails, select one type of authentication, and type the valid username and password.
   - **Host Name/Address:** Type the name of the mail server.
   - **Command Port:** Keep the default port 25, or modify it to match that of the mail server.
   - **SSL:** Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of Internet connection. When the option is enabled, the Command Port is changed to 465.
   - **Message Priority:** Assign the message a priority so the recipient knows to either look at it right away (high priority) or read it when time permits (low priority). A high priority message has an exclamation point next to it. Low priority is indicated by a down arrow.
   - **Send to:** Type a valid e-mail address and click the **Test** button to check if the server setup is correctly configured.

### 7.2.3 Setting Notification

1. On the menu bar, click **Tools** and select **Notifications**. This dialog box appears.

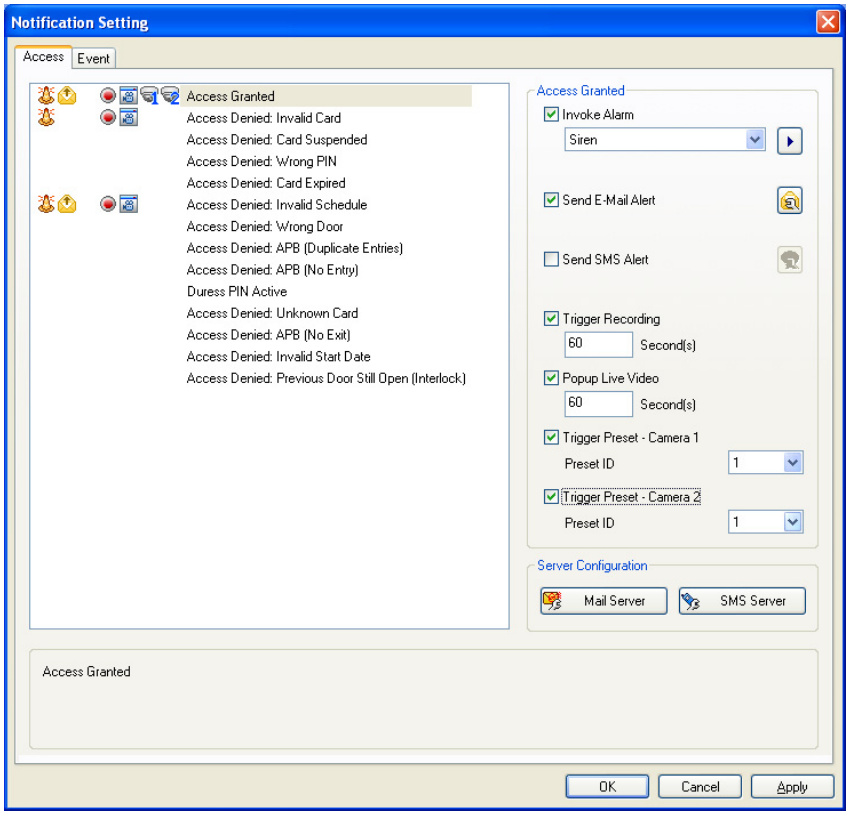



*Figure 7-6*

2. Use the **Access** and **Event** tabs to select one desired event for alert configuration.
3. Define the following alert approaches:
   - **Invoke Alarm:** Enable the computer alarm when the selected event occurs.
   - **Send E-Mail Alert:** When you select this option, an e-mail will pop up. Enter the recipient's e-mail address and alert subject. Then you can enter your own content, or use the buttons on the text window to send out the programmed information automatically.

     For example, if you click the  button, the sent SMS alert will include the controller information. For details see *C. E-Mail and SMS Alert Symbols* in *Appendix*.
   - **Send SMS Alert:** When you select this option, a dialog box will pop up. Ensure the preset mobile number(s). Select Text Code Type. Then type your messages; otherwise click the buttons on the text window to send out the programmed information automatically. See the above example in "Send E-Mail Alert".

- **Trigger Recording:** Enable recording of DVR, Video Server or Compact DVR when the selected event occurs. You can specify the recording time between 1 and 300 seconds. For the function to work, you must activate monitoring on these IP devices ahead.
- **Popup Live View:** An associated live view will pop up for alert when the selected event occurs. You can specify the duration of the live view remains on the screen between 1 and 300 seconds.
- **Trigger Preset:** Direct the camera(s) to a preset point when the selected event occurs.

4. To define more than one event with the same alert configuration, first right-click the previously defined event on the list and select **Copy** to save its settings. Then use Ctrl + left click or Shift + left click to select several events. Right-click the selected events and select **Paste** to have the same settings.

---

**Note:** For text code type, select **ASCII** for English that is limited to 160 characters and select **Unicode** for text of other languages that is limited to 70 characters.

---

## 7.3 Startup and Backup Setup

You can select which server should be enabled upon Windows or GV-ASManager startup.

You can also specify a path for the **Auto Backup** function to automatically save another copy of log and image files. The Auto Backup function performs backup at 24:00 A.M every day. By default, the log and image files are saved at **C:\Access Control\ASManager\ASBackup**.

- To access these functions, click **Tools** on the menu bar and select **Option**.

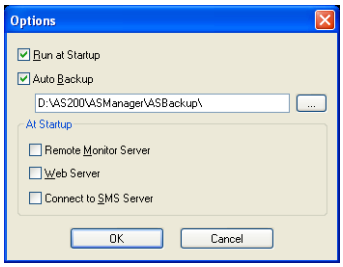



*Figure 7-7*

---

**Note:** To back up the Configuration files, see *11.3 Other Database Settings*.

---

## 7.4 Calendar System

You can select the calendar system of your country. The GV-ASManager supports these calendars: Hebrew, Japanese, Korean, Chinese Lunisolar, Persian, Taiwan and Thai Buddhist.

- To access this function, click **Tools** on the menu bar and select **Date Format**.

---

**Note:**

1. The Calendar System is not supported on Windows 2000.
2. For calendar system to work, it is required to install **Microsoft .NET Framework Version 3.5** from Software CD to the client PC.

---

## 7.5 Enrolling Fingerprints

GV-ASManager can work with **GeoFinger 1901** reader to enroll cardholders' fingerprints and transmit the fingerprint data to **GeoFinger 1901/1902** readers installed on GV-AS Controllers. To gain access the cardholder must present the enrolled fingerprint.

The wiring for this application is illustrated as below. GeoFinger 1901 reader installed on GV-ASManager is only for enrolling fingerprints. GeoFinger 1901/1902 readers installed on GV-AS Controllers receive the fingerprint data from GV-ASManager and verify the present fingerprint.

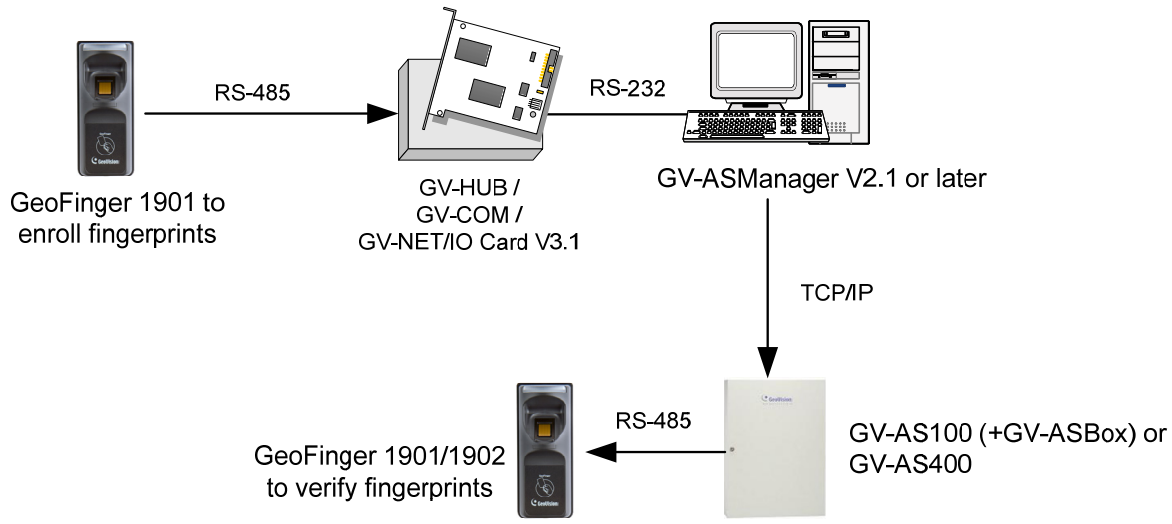



*Figure 7-8*

**Note:**

1. GV-AS200 does not support the fingerprint enrollment.
2. The fingerprint enrollment does not support the Wiegand connection.

### 7.5.1 Connecting to GeoFinger

The communication link between GeoFinger reader and the computer running GV-ASManager must be RS-485. For the RS-485 connection to the computer, a RS-485 to RS-232 converter, such as GV-COM, GV-Hub or GV-NET/IO Card, is required. Refer to Figure 7-8.

### 7.5.2 Enrolling Fingerprints

Before you start, you have to complete the card and cardholder enrollments. See *4.3 Setting Cards* and *4.6 Setting Cardholders.*

**Note:** If your GV-AS Controller is not equipped with any card readers, it is still required to enroll cards because each fingerprint needs to go along with a card number. In this case, you can create virtual card numbers to represent the enrolled fingerprints.

To enroll fingerprints:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Double-click one cardholder listed in the window. The Cardholder Setup dialog box appears.
3. Click the **Fingerprint** tab. This dialog box appears.

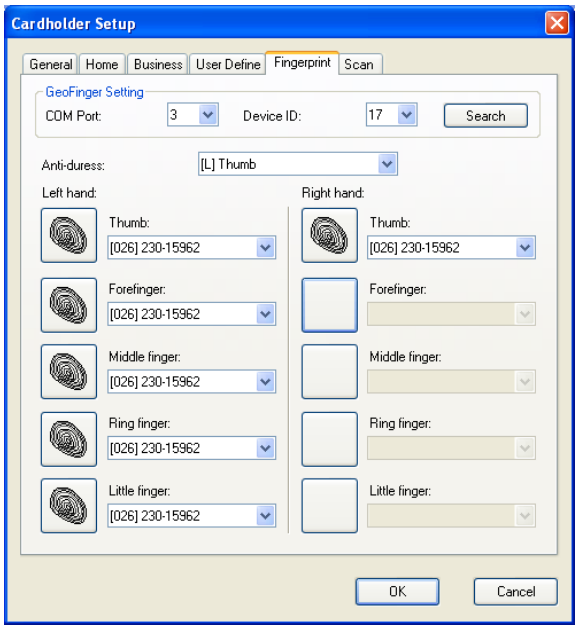



*Figure 7-9*

4. Click the **Search** button to detect the GeoFinger reader connected.
5. In the Left Hand and Right Hand sections, click any finger square to enroll the fingerprint.
6. Place the specific finger on the GeoFinger reader. It is required to register the same fingerprint twice to complete the enrollment. All the ten fingerprints of a cardholder can be enrolled.
7. Use the drop-down list to assign a card to the fingerprint.

8. To delete the enrolled fingerprint, place the mouse pointer on the desired fingerprint image. The button appears. Click the button to delete the fingerprint.
9. For the **Anti-duress** function, select a fingerprint from the Anti-duress drop-down list. When the cardholder is forced to open the door under threat, he can present the designated finger to activate an alarm and send a signal to the GV-ASManager for warning.
10. Click **OK** to apply the settings.

### 7.5.3 Uploading Fingerprints to Controllers

You can upload fingerprints to any Door/Gate installed with **GeoFinger 1901/1902** readers for access control. Each GeoFinger reader can store up to **1,900** fingerprints.

1. Ensure the GeoFinger reader has been set up on the GV-AS Controller. When the GeoFinger reader is detected on the GV-AS Controller, a green mark should appear in the **Setting Status** field on the GV-AS Controller's Web interface. See *GV-AS Controller Hardware Installation Guide*.

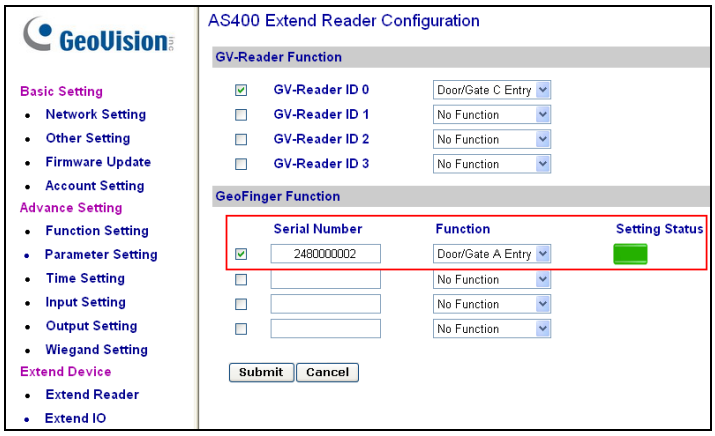



*Figure 7-10*

2. On the menu bar of GV-ASManager, click **Setup** and select **Fingerprint Access**. The Fingerprint Access dialog box appears.
3. Select the desired Controller and Door/Gate in the right pane.
4. Select the desired fingerprint data in the left pane. The **Add** button becomes available.
5. Click the **Add** button to upload the selected fingerprint data to the desired Door/Gate. When the uploading is complete, check marks will appear in the **In** (Enter) or **Out** (Exit) columns. The resulting window after uploading may look like this:

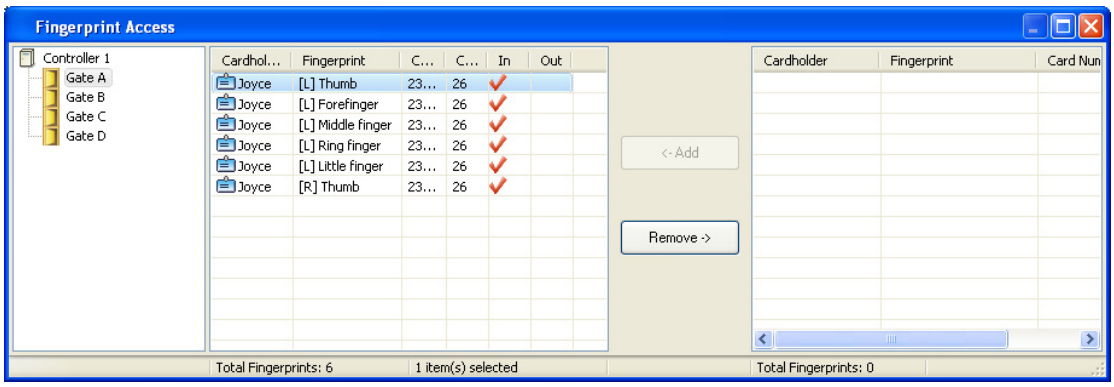



*Figure 7-11*

## 7.6 Scanning Driver's Licenses and Business Card

GV-ASManager can work with **SnapShell ID Scanner** to let you acquire and edit the personal data from driver's licenses and business cards.

---

**Note:** This function only supports SnapShell ID Scanner with SDK driver version.

---

1. Consult the Scanner's documentation to connect the Scanner with the GV-ASManager.
2. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List dialog box appears.
3. Click the **New** button. The Cardholder Setup dialog box appears.
4. Click the **Scan** tab. This dialog box appears.

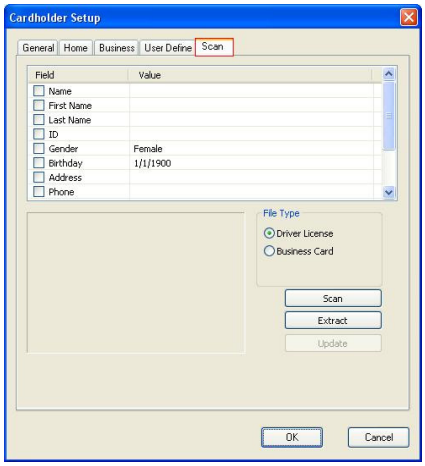



*Figure 7-12*

4. In the File Type field, select **Driver License** or **Business Card**. Here we use the Driver License as the example to demonstrate the following steps.

5. Place a driver's license on the Scanner and click the **Scan** button. The license image is displayed.

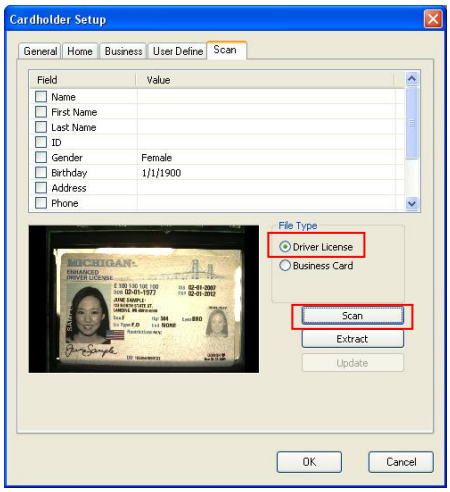



*Figure 7-13*

6. Click the **Extract** button to read the license data. The data is displayed in the **Value** column.
7. To modify the data, click the desired **Value** column and type the next texts. Click anywhere in the dialog box when you are finished with the modification.


*Figure 7-14*

8. Click the **Update** button. The data of this driver's license is saved to the GV-ASManager's database.
9. Now you can click the **Home** tab to view the information of the driver's license, or click the **Business** tab to view the information of the business card if scanned.

# Chapter 8 GV-ASLog

The GV-ASLog displays the event information of doors on the current day. The logs are displayed with access message, cardholder name, card number, door name and local time. You can also access images and play back video if available.

To use the GV-ASLog, the version of your browser must be **Internet Explorer 7 or later**.

To view the GV-ASLog:

1. To view the GV-ASLog, click **Tools** on the menu bar and select **ASLog**. This window appears.

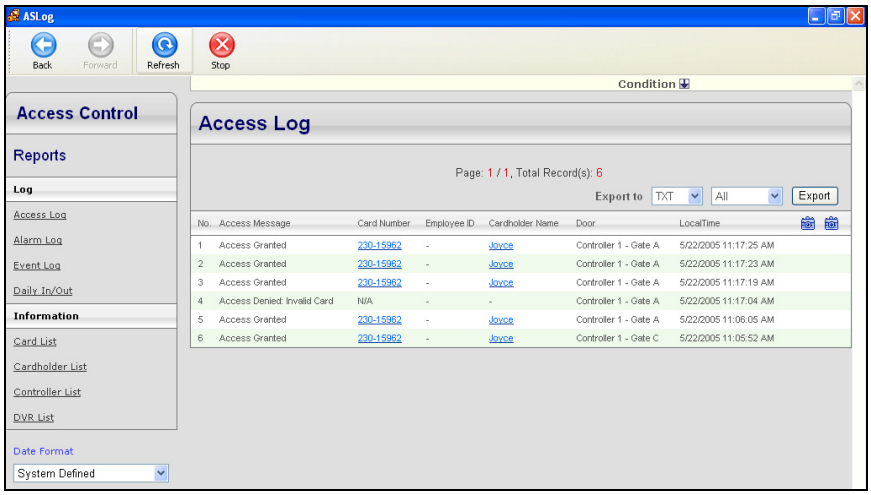



*Figure 8-1*

2. From the left pane, select the type of log, e.g. Access Log. The events for the current day are displayed according to your selection.
3. To view the logs of past days, click the Condition button. Then define search criteria to locate the desired events.
4. To export search results, click the **Export** button. Then save the results as **.txt**, **.xls** or **.htm** file.

Also see *10.2.1 Setting Search Criteria*, *10.2.2 Log Window Icons* and *10.2.4 Defining Columns*.

**Note:**

1. The GV-ASLog is not supported on Windows 2000.
2. You can play back video only when Remote ViewLog Service included in Control Center Server is enabled on the DVR. And the Remote ViewLog function is enabled on GV-Video Server or GV-Compact DVR.
3. To select a different calendar system from the Data Format list, see *Note* in *7.4 Calendar System* first.

# Chapter 9 GV-ASRemote

The client software GV-ASRemote is designed to monitor multiple GV-ASManagers over the network. The GV-ASRemote provides the following features:

- Remote monitoring
- Remote live view and playback
- Remote control: stop alarms and force the door to lock/unlock

## 9.1 Installing GV-ASRemote

Insert Software CD to your computer and a window will pop up automatically. Select **Install GeoVision V2.1 Access Control System**, click **GeoVision Access Control System** and follow on-screen instructions to complete the installation.

## 9.2 The GV-ASRemote Window

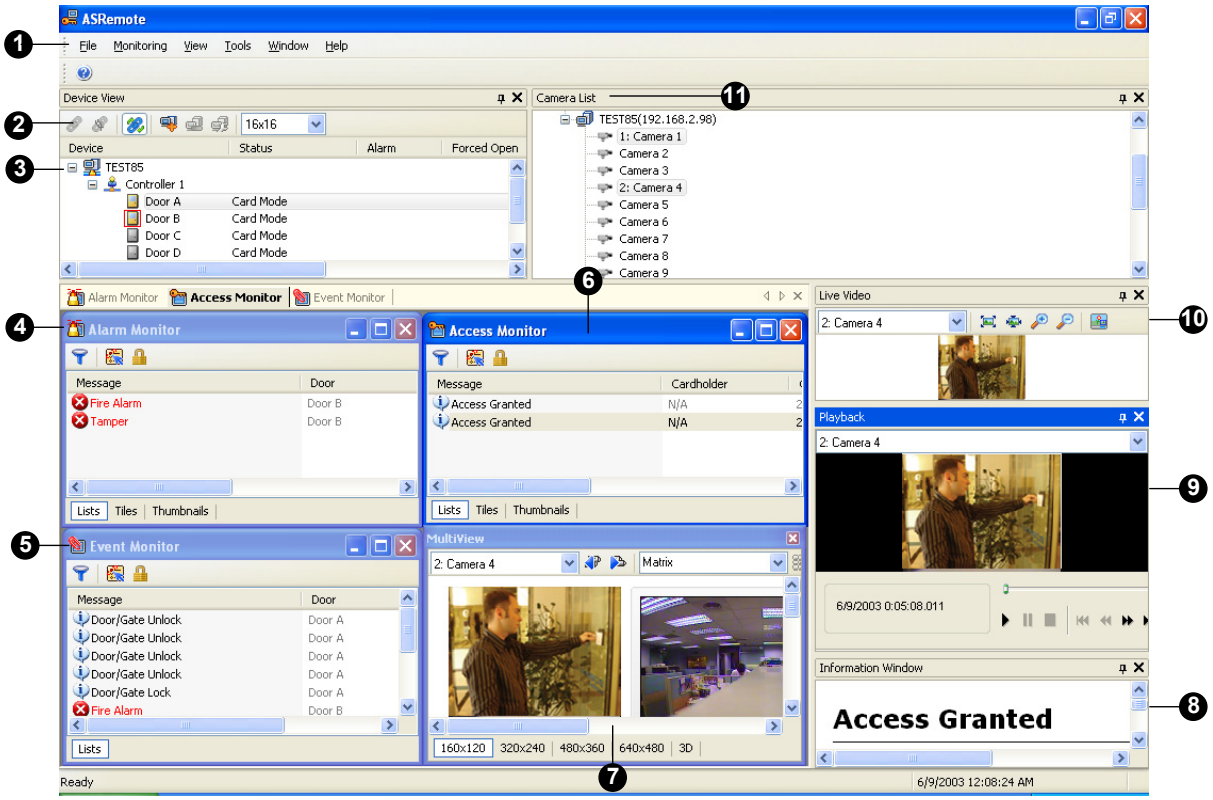



*Figure 9-1*

| No. | Name | Function |
|---|---|---|
| 1 | Menu Bar | The Menu Bar includes the options of **File** (log in / out the GV-ASManager), **Monitoring** (display monitor windows of alarm, access and event), **View** (display the function windows) and **Window** (arrange the display of different windows). |
| 2 | Toolbar | The Toolbar includes the options of **Connect**, **Disconnect**, **Auto Connect**, **Add Host**, **Remove Host**, **Settings** and **Resolution**. |
| 3 | Device View | Displays a list of connected doors and their current status. |
| 4 | Alarm Monitor | Displays alarm events of doors. |
| 5 | Event Monitor | Displays monitored events of doors. |
| 6 | Access Monitor | Displays access activities of doors. |
| 7 | MultiView | Displays live views of connected cameras from multiple IP devices. For details, see 5.4 The MultiView Window. |
| 8 | Information Window | Displays the information of doors, card readers and monitored events. |
| 9 | Playback | Plays back recorded events from a compatible GeoVision IP device. For details, see the same operations in 5.5 Retrieving Recorded Video. |
| 10 | Live Video | Displays live views of one connected camera. For details, see the same operations in 5.2 Accessing Live View. |
| 11 | Camera List | Displays a list of connected cameras. |

### 9.2.1 Toolbar

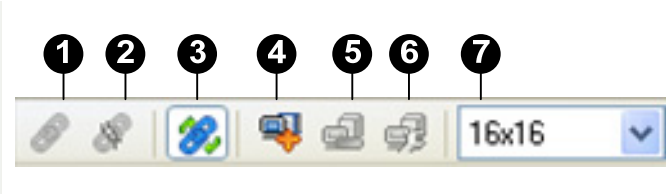



*Figure 9-2*

The buttons on the Toolbar of GV-ASRemote:

| No. | Name | Function |
|---|---|---|
| 1 | Connect | Starts the connection with the GV-ASManager. |
| 2 | Disconnect | Ends the connection with the GV-ASManager. |
| 3 | Auto Connect | Retries to build the connection with the GV-ASManager. |
| 4 | Add Host | Adds an GV-ASManager host to the list. |
| 5 | Remove Host | Deletes an GV-ASManager host on the list. |
| 6 | Settings | Edits the settings of GV-ASManager hosts. |
| 7 | Resolution | Changes the size of icons to 16 x 16, 24 x 24 or 32 x 32. |

## 9.3 Connecting to GV-ASManager

Before GV-ASRemote may connect to one GV-ASManager, the GV-ASManager must allow the remote access by this procedure:

- Click **Tools** on the menu bar, select **Servers** and enable **Remote Monitor Server**.

  When the server is started, the icon  appears at the bottom of the main screen.

To create a GV-ASManager host and enable connection to the GV-ASManager:

1. On the toolbar, click the **Add Host** button. This dialog box appears.

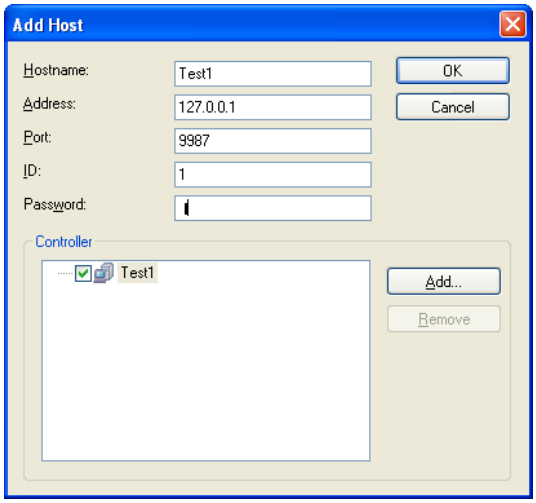



*Figure 9-3*

2. Give a hostname, type the GV-ASManager's IP address, modify the port number if necessary, and type the GV-ASManager's login ID and password.
3. Click **Add**. This dialog box appears.

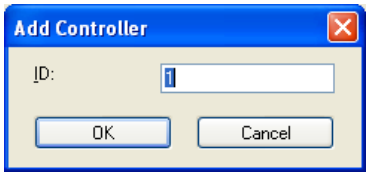



*Figure 9-4*

4. Type the ID of the controller associated with the GV-ASManager and click **OK.**
5. To add more controllers, repeat Steps 3-4.

6. Click **OK** and return to the main screen. A host folder will be displayed on the Device View window as example below.

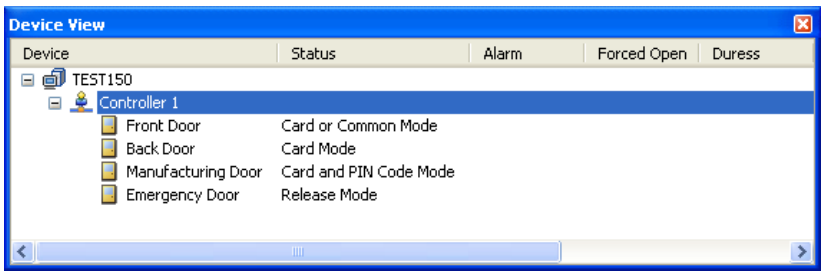



*Figure 9-5*

If the icon appears, it indicates the connection between GV-ASManager and GV-ASRemote has been established.

If the icon appears, it indicates the connection failed. Make sure GV-ASManager is enabled for the Remote Monitor Server function.

---

**Note:** For the disconnection messages displayed on the Status column (Figure 4-5), see *D. Controller Status* in Appendix.

---

# Chapter 10 GV-ASWeb

The GV-ASWeb is designed to query event data from the GV-ASManager over the network. With the connection to one GV-ASManager at a time, not only can users view event data but also download the logs in different formats.

To use the GV-ASWeb, the version of browser in the client PC must be **Internet Explorer 7 or later**.

## 10.1 Connecting to GV-ASManager

Before GV-ASWeb may connect to one GV-ASManager, the GV-ASManager must allow the remote access by this procedure:

- On the menu bar, click **Tools**, select **Servers** and enable **Web Server**. This dialog box appears.

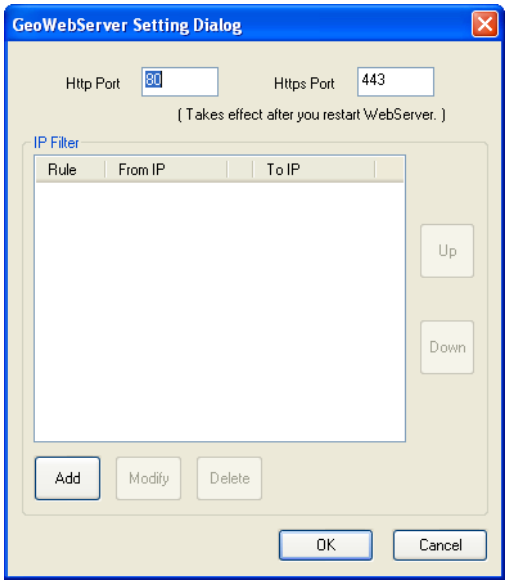



*Figure 10-1*

If you want to grant or deny the access from certain IP addresses, click **Add**, and type the IP addresses. Otherwise click **OK** to start the connection. When the server is started, the icon  appears at the bottom of the main screen.

To start the GV-ASWeb:

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected.

   This web page appears.

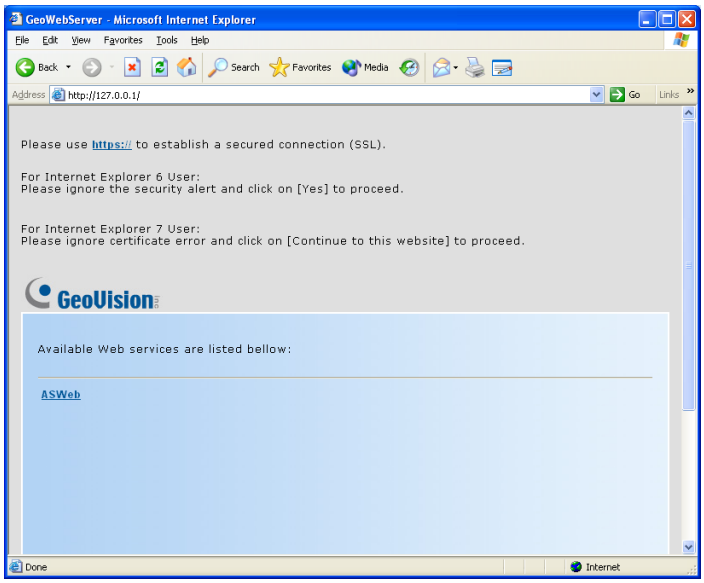



*Figure 10-2*

2. Click **https://** for SSL encrypted connection, or **ASWeb** for regular connection.
3. Enter a valid username and password for login. The GV-ASWeb page appears.

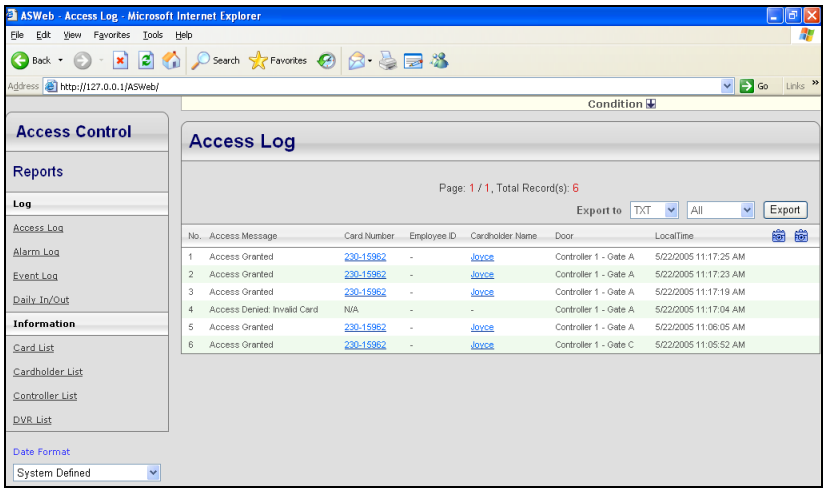



*Figure 10-3*

**Note:**

1. The GV-ASWeb is not supported on Windows 2000.
2. To select a different calendar system from the Data Format list, see *Note* in *7.4 Calendar System* first.

## 10.2 Accessing Logs

You can access the logs of the connected GV-ASManager, including Access Log, Card List, Cardholder List, Daily In/Out, Alarm Log, and Event Log. In addition, you can set up search criteria to view the records more efficiently.

### 10.2.1 Setting Search Criteria

1. Select a log from the left pane you want to view. Here we use Access Log as an example.
2. On the top of the log window, click the Condition button. A filter dialog box appears.
3. Type or select the desired filtering criteria. For example, we want to search the log for the records that match the conditions of “Access Granted”, Card Number “100012”, Front Door entrance (Dir. of In), and dates from August 20th to August 26th. The resulting filter window may look like this:

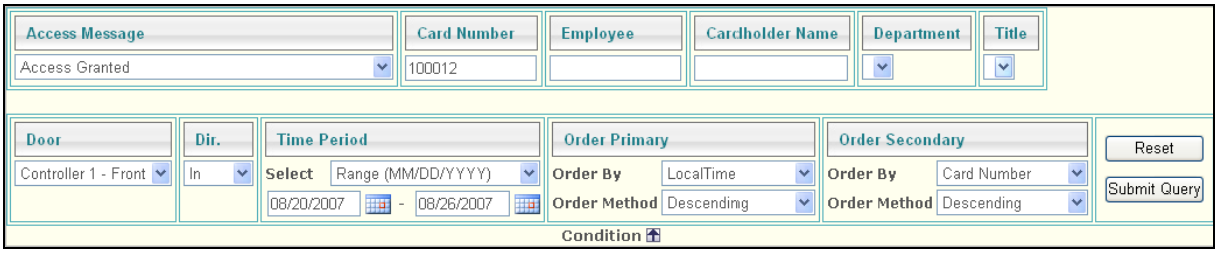



*Figure 10-4*

4. In both Order Primary and Order Secondary drop-down lists, select how the search results are sorted out and displayed on the screen.
5. In the View drop-down list, select **List** to display a list of search results, **List with Snapshot** to display a list of search results with associated video images, or **Snapshot Verification** to display the found video images along with cardholder photos in which way you can check if the card user and holder are identical. The size of the displayed image and photo is also selectable.
6. Click the **Submit** button to start the log search.

### 10.2.2 Log Window Icons

The icons on the log window can display the detailed information of that category. Click the icon to view the details.

 **:** Displays the card information.

 **:** Indicates the availability of the recorded video.

 **:** Indicates the availability of the video image.

---

**Note:** You can play back video only when Remote ViewLog Service included in Control Center Server is enabled on the DVR. And the Remote ViewLog function is enabled on Video Server or Compact DVR.

---

### 10.2.3 Exporting Logs

You can download the logs of the connected GV-ASManager to the current computer in three formats: **.txt**, **.htm** and **.xls**.

1. Use the drop-down list of Export to and select the file format **TXT**, **HTML** or **Excel**.
2. Use the next drop-down list to select **This Page** to save the current log page or **All** to save all logs.
3. Click **Export** to download the logs.

### 10.2.4 Defining Columns

You can define displayed columns for each type of log.

1. On the menu bar of the GV-ASManager, click **Tools** and select **ASWeb Field**. This dialog box appears.

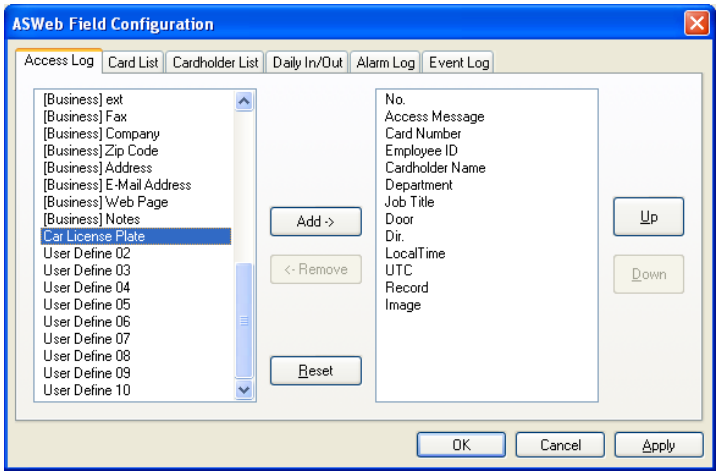



*Figure 10-5*

2. Click the desired log button, e.g. Access Log. The default columns are displayed on the right pane. Then use **Add** or **Remove** to define your log columns.

   For example, we added a user-defined field “Car License Plate” to the Access Log. The resulting window on the GV-ASWeb may look like this:

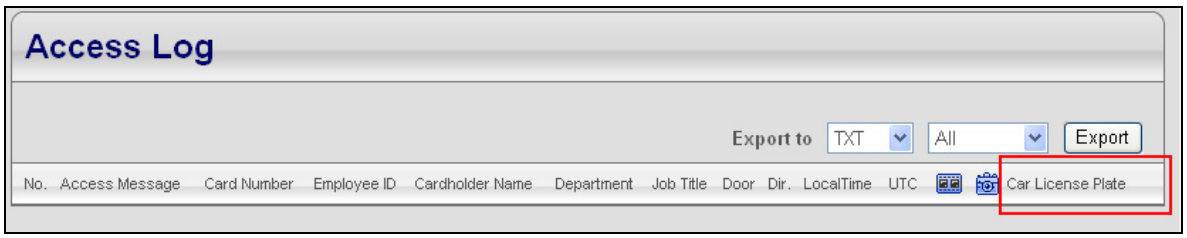



*Figure 10-6*

# Chapter 11 Database Settings

Before you can run GV-ASManager, it is required to create a database or to upgrade your old database to fit the latest version of GV-ASManager. You can select either a **Microsoft Office Access** or **Microsoft SQL Server** to be the database of GV-ASManager.

If a database already exits, the GV-ASManager provides you the **Source Database** function to convert various database formats to be the GV-ASManager's (Access or SQL Server).

## 11.1 Starting the Database Tools

To start the Database Tools, you may use one of the methods:

1. If you log in the GV-ASManager for the first time, this message will pop up: "*Cannot open database. Would you like to set up database?.* Click **Yes**. The following Database Tools dialog box will appear.
2. If you have run the GV-ASManager, run **ASDBManager.exe** from the program folder to access the Database Tools.

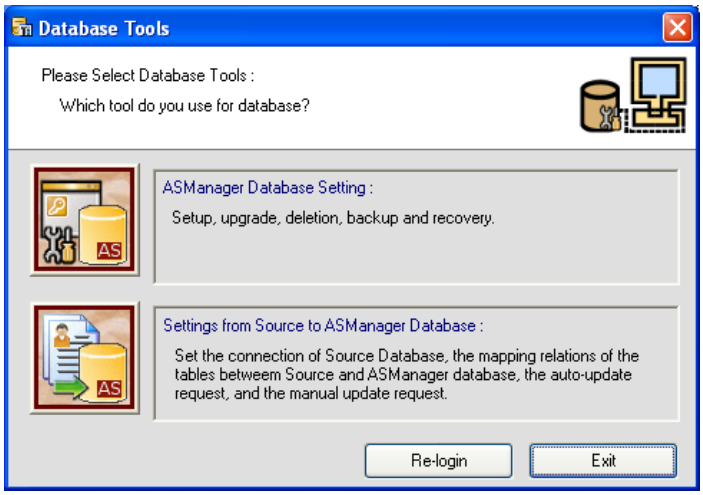



*Figure 11-1*

## 11.2 Creating a Database

You can select either Microsoft Office Access or Microsoft SQL Server as the database of GV-ASManager.

1. Click the **ASManager Database Setting** button on the Database Tools dialog box (Figure 11-1).
2. Click the **Setup MDB/MSSQL Database for ASManager** button. This dialog box appears.

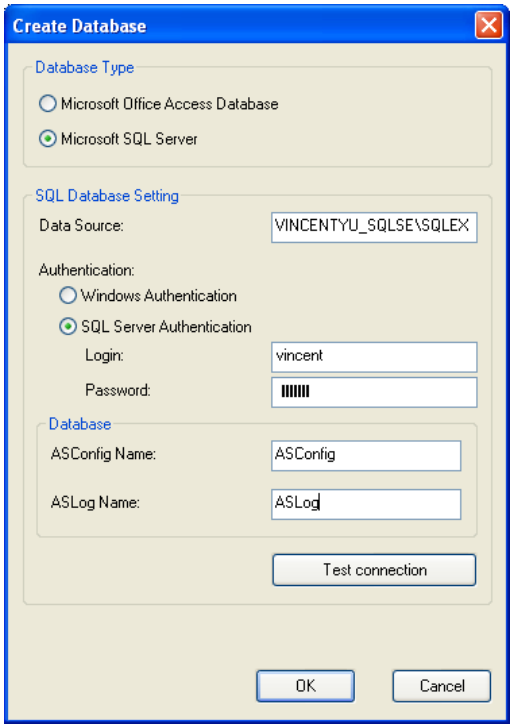



*Figure 11-2*

3. To use Access as the database, select **Microsoft Office Access Database** and click **OK**. The database is created in the local computer.
4. To use SQL Server as the database, select **Microsoft SQL Server.**
   a. Under the SQL Database Setting, type IP address or domain name of the SQL server in the Data Source field, and select its authentication way.
   b. Under the Database, name the databases for Configuration files and Log files that will be created on the SQL server separately.
   c. Click **Test Connection** to test the connection to the SQL server.
   d. Click **OK**. The databases are created in the SQL server.

## 11.3 Other Database Settings

You can upgrade, delete, back up and remove the database of GV-ASManager. Click **ASManager Database Setting** button on the Database Tools dialog box (Figure 11-1) to display the following dialog box and have further settings.


*Figure 11-3*

**[Upgrade to latest database version]** If an old database exits on the local computer, select this option to upgrade the version of the old database to the latest.

**[Delete ASManger Database]** Removes the database from the local computer or the SQL Server.

**[Backup Database]** Backs up the **Configuration** file.

**[Recovery Database]** Restores the backup **Configuration** file to the current computer or import it to another computer.

---

**Note:** To automatically back up Log and Image files, use the **Auto Backup** function. See *7.3 Startup and Backup Setup*.

---

## 11.4 Source Database Connection

The Source Database function can convert the databases of **OLE DB** and **Active Directory** to be the GV-ASManager's (Access or SQL Server). Click the **Setting from Source to ASManager Database** button on the Database Tools dialog box (Figure 11-1) to display the following dialog box and have further settings.

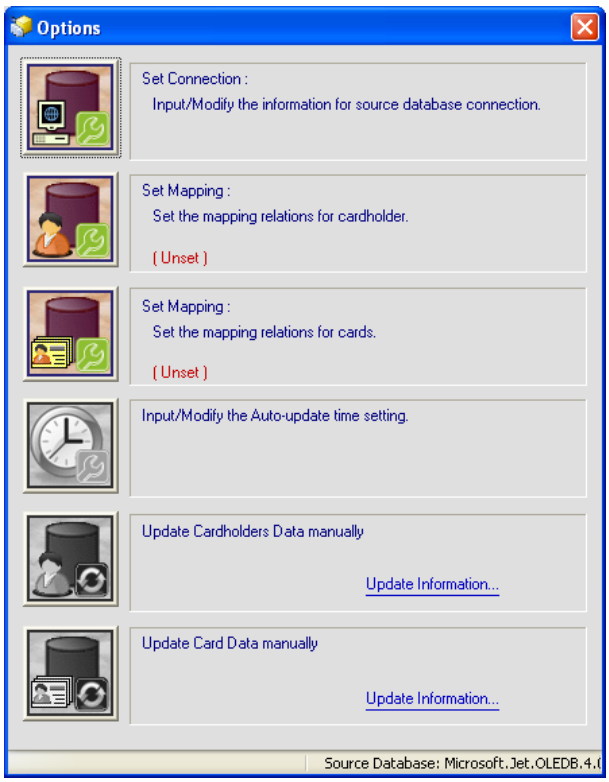



*Figure 11-4*

**[Set Connection]** Configures the connection to an active directory or an OLEDB provider.

**[Set Mapping….for cardholder]** Maps the cardholder fields between the GV-ASManager database and the source database.

**[Set Mapping….for card]** Map the card fields between the GV-ASManager database and the source database.

**[Input/Modify the auto-update time setting]** Specify a time to update the database automatically.

**[Update Cardholders Data manually]** Update the cardholder data manually.

**[Update Card Data manually]** Update the card data manually.

### 11.4.1 Converting Data from the Active Directory Database

1. Click the **Set Connection** button on the Options dialog box (Figure 11-4). The Source Database dialog box appears.
2. Select **Active Directory**. This dialog box appears.

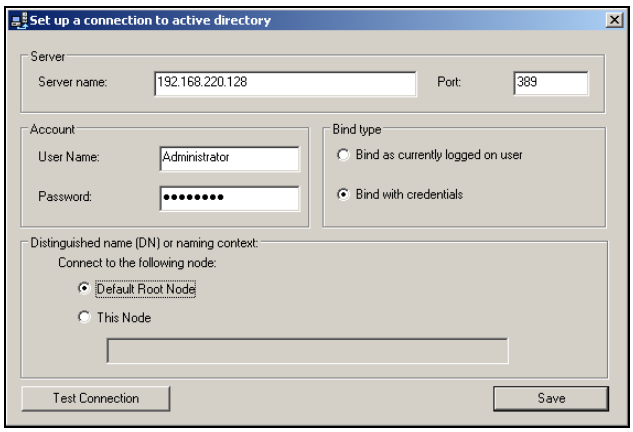



*Figure 11-5*

3. If you log in the local computer with the authorized username and password from the source database server, select **Bind as currently logged on user** and type the IP address or domain name of the server. If not, select **Bind with credentials**, type the IP address or domain name of the server and its login username and password.
4. Ensure the **Port** number matches that of the source database server.
5. Select **Default Root Node** to connect to the root node of the source database. Otherwise, select **This Node** and specify the node path.
6. Click **Test Connection** to connect to the source database server.
7. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 11-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
8. Click the **Update Card Data manually** button in the Options dialog box (Figure 11-4) to convert the card data from the source database to the GV-ASManager database immediately.
9. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 11-4) and specify the time in minutes.

### 11.4.2 Converting Data from the OLE Database

To convert data from the OLE database, you need to go through these instructions:

- **Connect an OLE database**
- **Map the cardholder data**
- **Map the card data**
- **Convert the data from the source database**

### To connect an OLE database:

1. Click the **Set Connection** button on the Options dialog box (Figure 11-4). The Source Database dialog box appears.
2. Select **Other Database**. This dialog box appears.

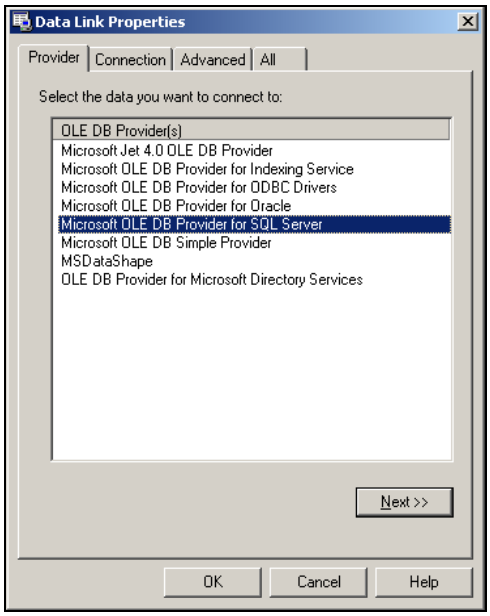



*Figure 11-6*

3. Select the OLE DB provider that you wish to connect to, and click **OK**. The connection dialog box appears. The dialog box varies depending on the OLE DB provider you choose. Here we select **Microsoft OLE DB Provider for SQL Server** as example.

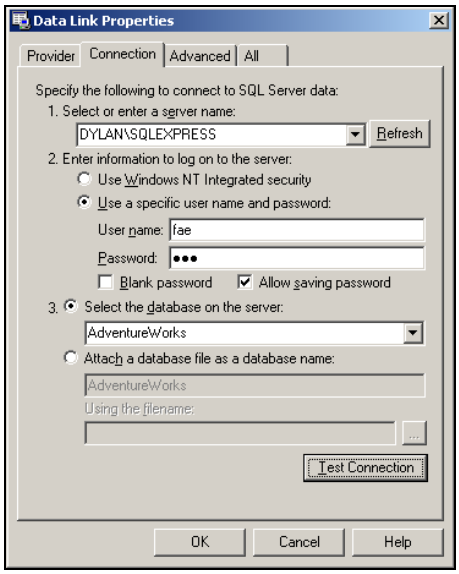



*Figure11-7*

4. Type the IP address or domain name of the source database server, select its login authentication method, and select a specific database on the server. Click **Test Connection** to connect to the source database server.

## To map the cardholder data:

1. Click the **Set the mapping relations for cardholders** button in the Options dialog box (Figure 11-4). This window appears.

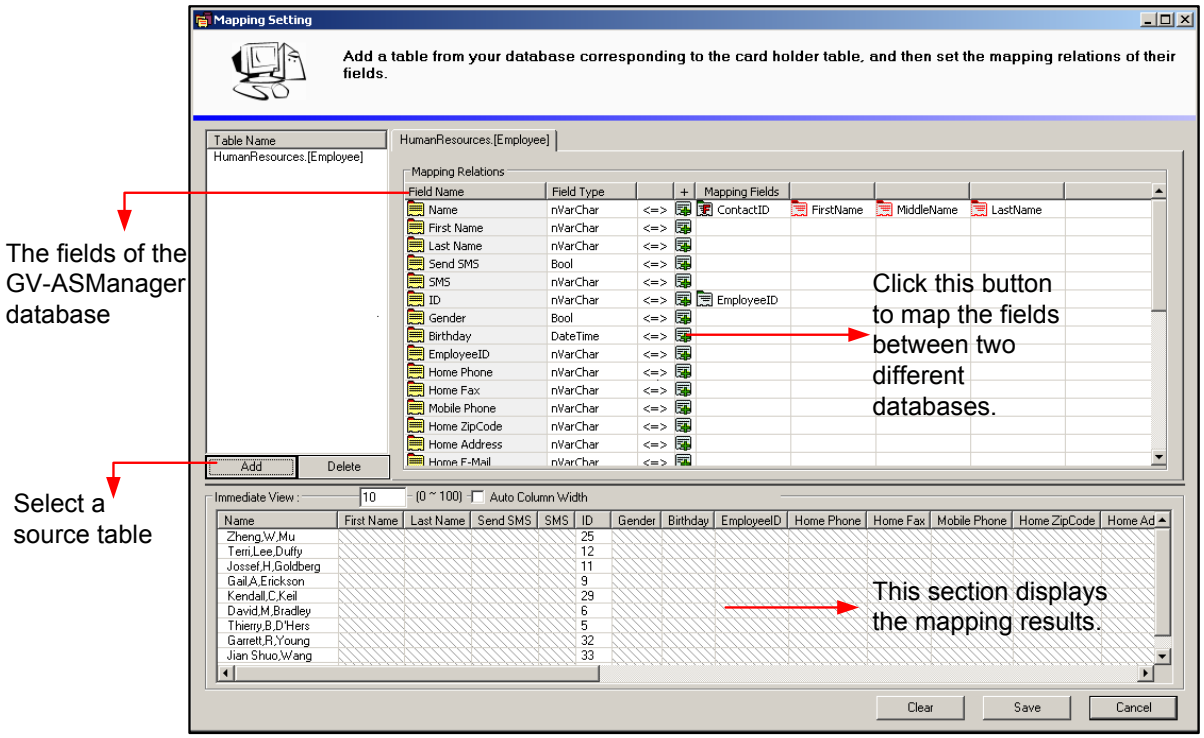



*Figure 11-8*

2. Click the **Add** button to select a related table on the source database.
3. Click the buttons to map each field of GV-ASManager database to a corresponding field of the source database.
4. In the following steps, we demonstrate how to map the **Name** filed as example. Click the button in the Name field. This dialog box appears.

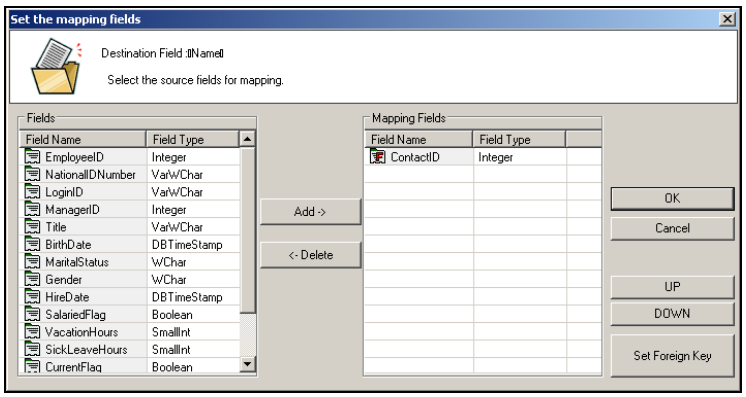



*Figure 11-9*

5. In the left side of the mapping field dialog box, select the field(s) of the source database corresponding to the Name field of the GV-ASManager database. Then click **Add**. In this example (Figure 11-9), the **Contact ID** field of the source database corresponds to the **Name** filed of the GV-ASManager database.

6. If the field of the source database, without having the data entered, is linked to an index or another table, click the **Set Foreign Key** button. This dialog box appears.

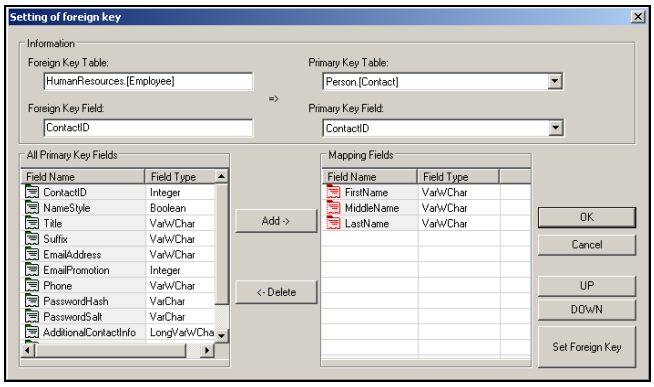



*Figure 11-10*

7. When the foreign key dialog box is open, the linked **Primary Key Table** and **Primary Key Field** should be displayed if the connection of the Foreign Key Table and Primary Key Table has been created. Otherwise, use the drop-down lists to select the Primary Key Table and Field.

8. In the left side of the foreign key dialog box, select the field(s) of the Primary Key Table corresponding to the field of the Foreign Key Table. In this example (Figure 11-10), the **Contact ID** field of “Human Resource (Employee)” Foreign Key Table is linked to the **First Name**, **Middle Name** and **Last Name** fields of “Person (Contact)” Primary Key Table.

9. Click **OK**. In the Mapping Setting window, you can see the mapping results. In the example (Figure 11-8), the **Name** field of the GV-ASManager database is mapped to the **Contact ID** field of the source database which includes **First Name**, **Middle Name** and **Last Name** (which are linked from the Primary Key Table).

## To map the card data:

1. Click the **Set the mapping relations for cards** button in the Options dialog box (Figure 11-4). This window appears.

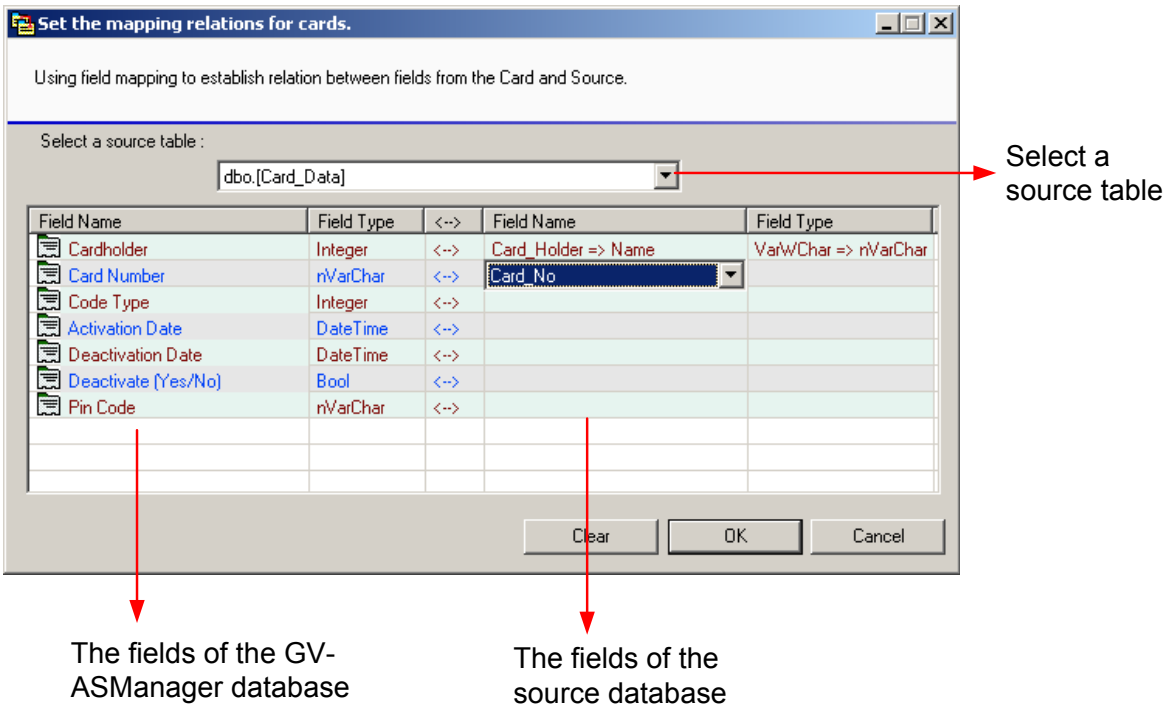



*Figure11-11*

2. Select a related table on the source database.
3. Click the **Field Name** column on the right side to map each field of the GV-ASManager database and the source database.

## To convert the data from the source database:

1. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 11-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
2. Click the **Update Card Data manually** button in the Options dialog box (Figure 11-4) to convert the card data from the source database to the GV-ASManager database immediately.
3. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 11-4) and specify the update time.

# Chapter 12 Net Module Utility

With the **Net Module Utility** included in Software CD, you can change settings and update the firmware of the GV-AS Controller.

1. Insert Software CD, select **Install GeoVision V2.1.0.0 Access Control System**, click **Net Module Utility** and follow the onscreen instructions to install the program.
2. Run **Net Module Utility**. This window appears.

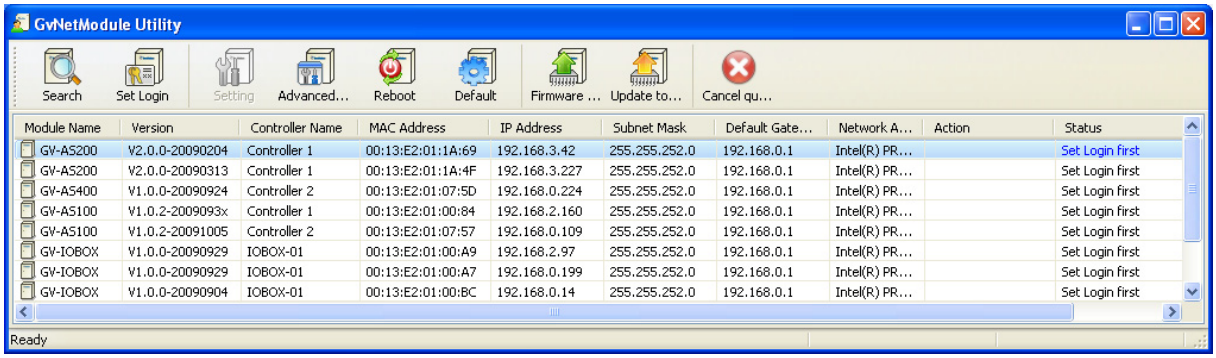



*Figure 12-1*

The buttons on the window:

- **Search:** Click this button to locate any GV-AS Controller or GV-I/O device on the same LAN.
- **Set Login:** You can select the desired modules from the list, and click this button to log on to these modules with the same ID and password together.
- **Setting:** Click this button to change the Machine Name, IP address, 3DES Code, Device Port, login ID and password.
- **Advanced Setting:** Click this button to directly link to the Web interface of the selected module.
- **Reboot:** Click this button to perform a warm boot of the selected module. This operation will keep the current configuration.
- **Default:** Click this button to resets all configuration parameters to their factory settings. This may take 5 seconds to complete.
- **Firmware Update:** Click this button and assign the firmware file for update.
- **Update to the latest firmware version:** The GV-ASManager software comes with the latest GV-AS Controller firmware. Clicking this button can upgrade your GV-AS Controller firmware.

# Chapter 13 Troubleshooting

## Q1: GV-ASManager cannot connect to GV-AS Controller over the Internet.

There are several causes for this problem such as IP address conflict, incorrect connection settings and network failure. The following solution is to assign the fixed IP to the GV-ASManager and GV-AS Controller respectively. This way can determine if the problem is caused by the faulty devices and incorrect network settings.

1. Disconnect the hub or switch, which connects the GV-ASManager and GV-AS Controller, from the network.
2. Give the GV-ASManager a fixed IP address that is NOT used by another device, e.g. 192.168.0.154.

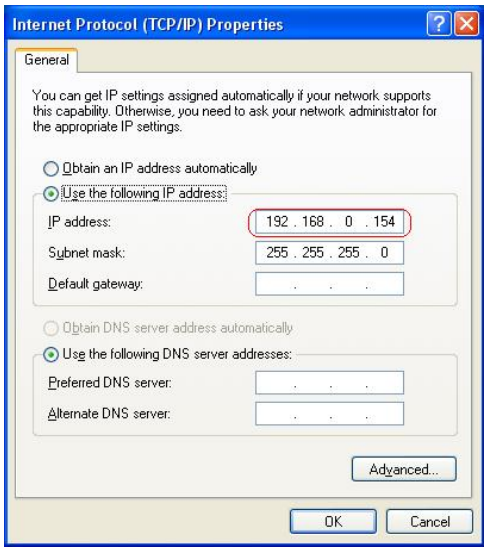



*Figure 13-1*

3. Reset the GV-AS Controller module and Ethernet module to factory defaults.
   a. Plug the GV-ASKeypad to the GV-AS Controller.
   b. Remove the jumper cap from the 2-pin **Default** jumper.
   c. Press the **Reset** button.
   d. Replace the jumper cap back to the 2-pin **Default** jumper.
   e. To reset the Ethernet Module, press and hold the **Default EN** button for 6 seconds.
4. Open the browser and enter the GV-AS Controller default address: http://192.168.0.100

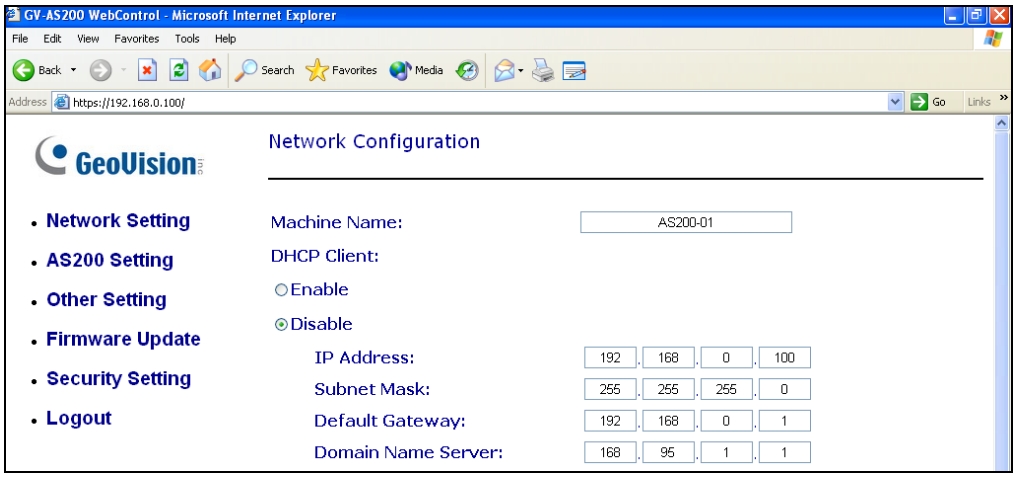



*Figure 13-2*

5. In the IP address field, give the GV-AS Controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
6. On the GV-ASManager, enter the following settings:

   **Controller ID:** 1

   **Network:** TCP/IP

   **IP:** 192.168.0.XXX

   **Port:** 4000

   **User:** admin

   **Password:** 1234

   **Crypto key:** 12345678

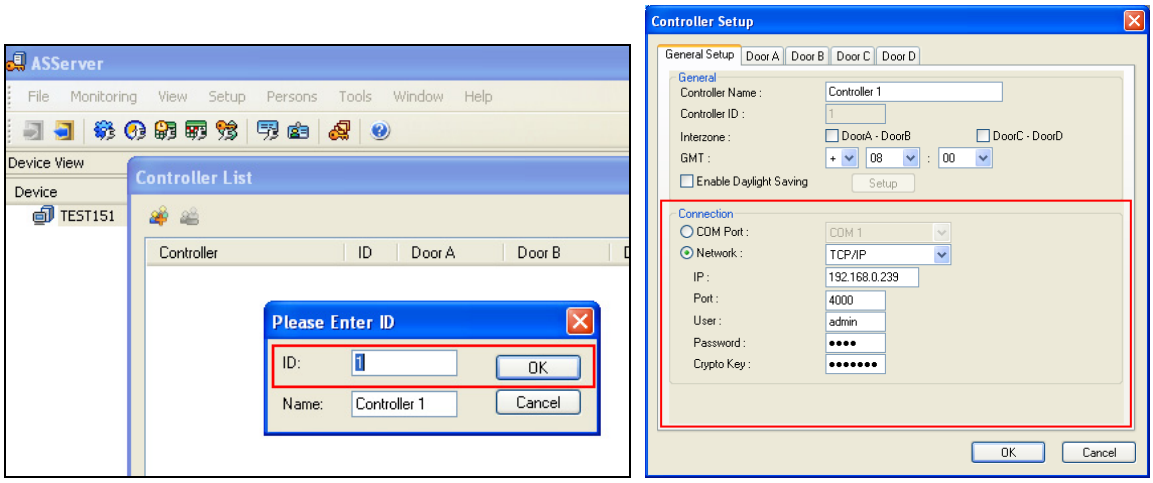



*Figure 13-3*

7. The connection between the GV-ASManager and GV-AS Controller should be established, and the connection icon should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

## Q2: The connection established between the GV-ASManager and GV-AS Controller is interrupted.

This may be due to IP address conflict. Follow these steps to troubleshoot the problem:

1. Disconnect the hub or switch, which connects to the GV-ASManager and GV-AS Controller, from the network.
2. Run Windows **Command Prompt**. Take Classic Windows Start Menu for example, click **Start**, select **Accessories** and click **Command Prompt**.
3. Type **arp –d** and press **Enter**.

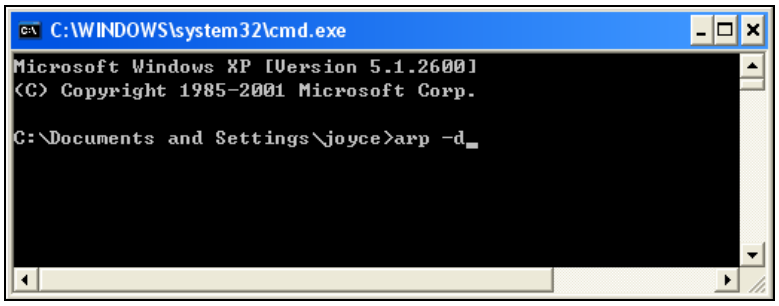



*Figure 13-4*

4. Give the GV-ASManager a fixed IP address that is NOT used by another device. See Figure 10-1.
5. Open the browser and enter the assigned IP address of GV-AS Controller. The Network Configuration page appears. See Figure 10-2.
6. In the IP address field, give the GV-AS Controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
7. On the GV-ASManager, enter the following settings. See Figure 10-3

   **Controller ID:** 1

   **Network:** TCP/IP

   **IP:** 192.168.0.XXX

   **Port:** 4000

   **User:** admin

**Password:** 1234

**Crypto key:** 12345678

8. The connection between the GV-ASManager and GV-AS Controller should be established, and the connection icon  should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

### Q3: GV-ASManager cannot receive card messages but the reader accepts the card when the connection between the GV-ASManager and GV-AS Controller is well established.

It may be due to memory failure in the GV-AS Controller. Reset both the GV-AS Controller module and the Ethernet module to factory settings. Refer to Step 3 in Question 1.

### Q4: The GV-ASManager cannot retrieve the video from the DVR for playback.

1. Make sure the **Remote ViewLog Service** on **Control Center Server** is enabled on the DVR.
2. Make sure the time on the GV-ASManager and the DVR is consistent.
3. Make sure the event file you want to play back has been created completely on the DVR. For example, the assigned time length of every recorded event on the DVR is 5 minutes. The desired event of 5 minutes must have been displayed on the ViewLog Event List, so you can access the event file for playback.

### Q5: After I add a card by presenting to the reader, the message "*Access Denied Invalid Card*" still appears

(For details on adding a card, see Step 1 in *4.3.1 Adding a Single Card.)*

It may be the card format is not compatible with the GV-AS Controller. For GV-AS200, ensure the format of your card reader is a Wiegand device of 26~40 bits; for GV-AS100 and GV-AS400, ensure the format is 26~64 bits. Otherwise, send us the related information of your card format so that we can customize the format for you.

## Q6: The GV-ASManager cannot receive card messages from the GV-Reader connected to the GV-AS Controller through RS-485 interface.

1. Make sure the GV-Reader is correctly wiring to the GV-AS Controller and Switch 4 on the GV-Reader is set to OFF.
2. Make sure the correct GV-Reader ID is set on the GV-AS Controller. Take GV-AS200 as example:
   a. Plug the GV-ASKeypad to the GV-AS Controller.
   b. Press any button on the keypad, select **Set Parameter**, and press the ENT YES button.
   c. Enter the default password **1234**, and select **Set GV-Reader ID** by using the UP and DOWN arrow buttons.
   d. Change GV-Reader ID 0 to **Extended Wiegand**.

## Q7: How to let all doors open when the fire situation is detected by GV-AS200.

Follow these steps for wiring on the GV-AS200 Controller and setting on the GV-ASManager:

1. Connect two Fire pins of Door A and Door B together. (illustrated as Red line)
2. Connect two GND pins of Door A and Door B together. (illustrated as Black line)
3. Connect the fire detector to both Fire and GND pins of Door A (illustrated as Green line)
4. Connect the fire detector to both Fire and GND pins of Door B (illustrated as Purple line)

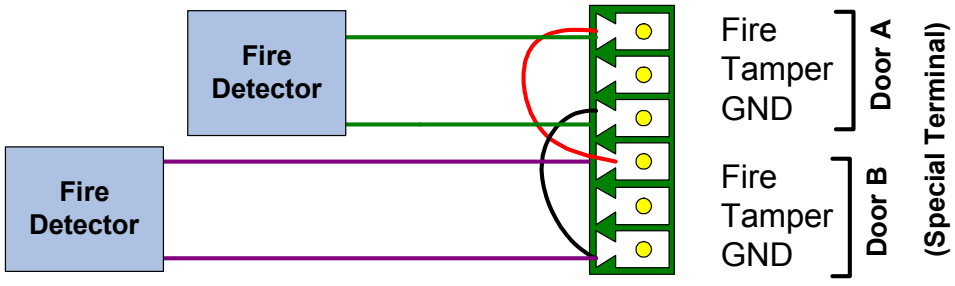



*Figure 13-5*

5. In the Controller Setup dialog box, click the **Door A** and **Door B** tab respectively, and select **Unlock Door** in the Fire Action option.

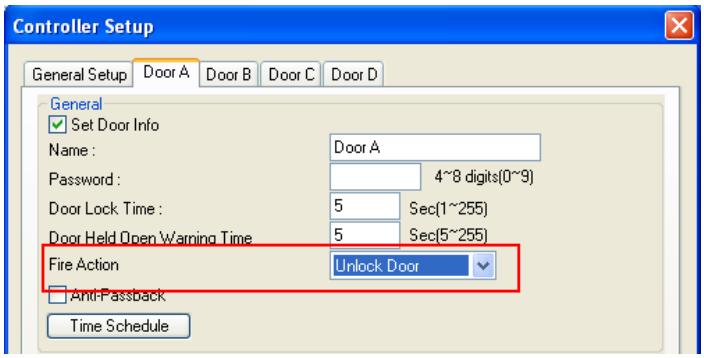



*Figure 13-6*

## Q8: How can I find more help?

Visit our website at http:///www.geovision.com.tw

Write us at support@geovision.com.tw

# Appendix

## A. Compatible IP Devices

**Arecont Vision**

| Model |
|---|
| AV1300 |
| AV2100 |
| AV3100 |
| AV3130 |
| AV5100 |
| AV5105 |

**AXIS**

| Model |
|---|
| 213 |
| 214 |
| 215 |
| 216FD |
| 216FD-V |
| 216MFD |
| 216MFD-V |
| 221 |
| 223M |
| 225FD |
| 231D+ |
| 232D+ |
| 233D |
| 241Q |
| 241S |
| P3301 |
| Q7401 |

**Canon**

| Model |
|---|
| VB-C50i |
| VB-C300 |

**IQEye**

| Model |
|---|
| 301 |
| 302 |
| 510 |
| 511 |
| 701 |
| 702 |
| 703 |
| 705 |
| 752 |
| 753 |
| 755 |

**JVC**

| Model |
|---|
| 301 |
| 302 |
| 510 |
| 511 |
| 701 |
| 702 |
| 703 |
| 705 |

**Mobotix**

| Model |
|---|
| M12D Sec-DNight |
| M12D Web |
| M12D IT-DNight |
| M12D Sec |
| M12D Sec-R8 |

**Panasonic**

| Model |
|---|
| BB-HCE481A |
| BB-HCM110 |
| BB-HCM311 |
| BB-HCM331 |
| BB-HCM371 |
| BB-HCM381 |
| BB-HCM403 |
| BL-C10 |
| BL-C30 |
| WV-NS202A |
| WV-NW484 |
| WV-NW964 |

**Pelco**

| Model |
|---|
| IP110 Series |
| IP3701Series |

**SONY**

| Model |
|---|
| SNC-CM120 |
| SNC-CS10 |
| SNC-CS11 |
| SNC-CS20 |
| SNC-CS50N |
| SNC-CS50P |
| SNC-DF40N |
| SNC-DF40P |
| SNC-DF50N |
| SNC-DF50P |
| SNC-DF70N |
| SNC-DF70P |
| SNC-DF80N |
| SNC-DF80P |
| SNC-DM110 |
| SNC-DM160 |
| SNC-DS10 |
| SNC-DS60 |
| SNC-P1 |
| SNC-P5 |
| SNC-RX530N |
| SNC-RX530P |
| SNC-RX550N |
| SNC-RX550P |
| SNC-RX570N |
| SNC-RX570P |
| SNC-RZ25N |
| SNC-RZ25P |
| SNC-RZ50N |
| SNC-RZ50P |

# B. Event Notifications

- **"Alarm" events**

| Type | Description |
|---|---|
| Force Open | Door <name> is forcibly open. |
| Duress | Duress function is triggered.<br>See "Duress" in *1.2 Concepts*. |
| Tamper | Tamper Inputs are triggered.<br>For hardware settings, see *Connecting Input Devices* in GV-AS Controller Hardware Installation Guide.<br>For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*. |
| Fire Alarm | Fire Inputs are triggered.<br>For hardware settings, see *Connecting Input Devices* in GV-AS Controller Hardware Installation Guide.<br>For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*. |
| Held Open | Door <name> is held open over the specified time.<br>See Step 2 and 5 in *4.2.2 Step 2: Configuration a Door.* |
| Access Denied | The access is rejected. |

- **"Access" events**

| Type | Description |
|---|---|
| Access Granted | The access from Cardholder <name> and Card <Number> is granted. |
| Access Denied: Invalid Card | The access is rejected because an unknown card is presented. |
| Access Denied: Card suspended | The access is rejected because Card <Number> is suspended. |
| Access Denied: Wrong PIN | The access is rejected because the PIN number entered is wrong. |
| Access Denied: Card Expired | The access is rejected because Card <Number> is expired. |
| Access Denied: Invalid schedule | The access is rejected because the user access is not on the programmed schedule. |
| Access Denied: Wrong Door | The access is rejected because the user has access to the wrong door. |

| | |
|---|---|
| Access Denied: APB (Duplicate Entries) | The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as successive entries, without exit, to a secure area. |
| Access Denied: APB (No Entry) | The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as exit, without entry, to a secure area. |
| Access Denied: APB (No Exit) | The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as entry, without exit, to a secure area. |
| Access Denied: Unknown Card | The access is rejected because the card format is not compatible. |
| Access Denied: Invalid Start Date | The access is rejected because Card <Number> is not enabled. |
| Access Denied: Previous Door Still Open (Interlock) | The access is rejected because the Interlock function is violated. The entry door is left unlocked.<br>See “Interlock” at Step 5 in *4.2.1 Step 1: Configuring a Door Controller*. |

- **“Event” events**

| Type | Description |
|---|---|
| Force Open | Door <name> is forcibly open. |
| Duress | Duress function is triggered.<br>See “Duress” in *1.2 Concepts*. |
| Tamper | Tamper Inputs are triggered.<br>For hardware settings, see *Connecting Input Devices* in GV-AS Controller Hardware Installation Guide.<br>For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*. |
| Fire Alarm | Fire Inputs are triggered.<br>For hardware settings, see *Connecting Input Devices* in GV-AS Controller Hardware Installation Guide.<br>For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*. |
| Held Open | Door <name> is held open over the specified time.<br>See Step 2 and 5 in *4.2.2 Step 2: Configuration a Door.* |
| Access Denied | The access is rejected. |
| Alarm Restored | Alarm sounds are cleared. |
| Forced Open-Restored | Force Open alarm is cleared. |

| | |
|---|---|
| Duress Restored | Duress alarm is cleared. |
| Tamper Restored | Tamper alarm is cleared. |
| Fire Alarm Restored | Fire alarm is cleared. |
| Held Open Restored | Held Open alarm is cleared. |
| Restored Alarm Failed | Fail to clear alarm sounds. |
| Clear Forced Open Event Failed | Fail to clear Force Open alarm. |
| Clear Duress Event Failed | Fail to clear Duress alarm. |
| Clear Tamper Event Failed-No Event Present | Fail to clear Tamper alarm. |
| Clear Fire Alarm Event Failed-No Event Present | Fail to clear Fire alarm. |
| Clear Held Open Event Failed | Fail to clear Held Open alarm. |
| Clear Access Denied Failed | Fail to clear Access Denied alarm. |
| Clear Tamper Event Failed-I/O Still Unclear | Fail to clear Tamper alarm because Tamper Inputs remain triggering. |
| Clear Fire Event Failed-I/O Still Unclear | Fail to clear Fire alarm because Fire Inputs remain triggering. |
| Door Open | Door <name> is open. |
| Door Close | Door <name> is close. |
| Door/Gate Unlock | Door <name> is unlocked. |
| Door/Gate Lock | Door <name> is locked. |
| Two Person Rule-Active | Two-person A/B rule is active when Card <number> is presented. |
| Two Person Rule-Confirm | Two-person A/B rule is confirmed when Card <name> is presented after the other AB card. |
| Two Person Rule-Inactive | Two-person A/B rule is violated when Card <name> is presented successively or the other AB Card isn't presented within 20 seconds. |
| Keypad Code Confirm | On the Card or Common mode, the password entered is correct. |
| Wrong Keypad Code | On the Card or Common mode, the password entered is wrong. |

| | |
|---|---|
| Release Mode | Door <name> is on the Release Mode.<br>See Step 4 in *4.2.2 Step 2: Configuration a Door*. |
| Card or Common Mode | Door <name> is on the Card or Common Mode.<br>See Step 4 in *4.2.2 Step 2: Configuration a Door*. |
| Card and PIN Code Mode | Door <name> is on the Card and PIN Code mode.<br>See Step 4 in *4.2.2 Step 2: Configuration a Door*. |
| Card Mode | Door <name> is on the Card mode.<br>See Step 4 in *4.2.2 Step 2: Configuration a Door*. |
| Fire Unlock Mode | Door <name> is unlocked after Fire Inputs are triggered.<br>See “Fire Action” at Step 2 in *4.2.2 Step 2: Configuration a Door*. |
| Fire Lock Mode | Door <name> is locked after Fire Inputs are triggered.<br>See “Fire Action” at Step 2 in *4.2.2 Step 2: Configuration a Door*. |
| Force Unlock Remotely | Door <name> is unlocked remotely from the control of GV-ASManager or GV-ASRemote server. |
| Force Lock Remotely | Door <name> is locked remotely from the control of GV-ASManager or GV-ASRemote server. |
| Disable Remote Door Lock Operation | The event of “Force Unlock Remotely” or “Force Lock Remotely” is cleared. |
| Force Unlock Locally | Door <name> is unlocked on the site of Door Controller. |
| Force Lock Locally | Door <name> is locked on the site of Door Controller. |
| Disable Local Door Lock Operation | The event of “Force Unlock Locally” or “Force Lock Locally” is cleared. |
| Reset | Door Controller <name> is reset. |

## C. E-Mail and SMS Alert Symbols

| Icon | Description |
|---|---|
|  | %M (Message): include related alert message. |
|  | %T (Controller): include door controller's name. |
|  | %D (Door): include triggered door's name. |
|  | %L (Local Time): include local time. |
|  | %U (UTC): include UTC time. |
|  | %N (Card Number): include card number. |
|  | %H (Card Holder Name): include cardholder name. |
|  | %G (Gender): include cardholder's gender. |
|  | %E (Employee ID): include employee ID. |
|  | %Y (Company): include company name. |
|  | %P (Department): include department name. |
|  | %F (Office): include office name. |
|  | %C (Photo): include cardholder photo |
|  | %S (Snapshot): include snapshot. |

# D. Controller Status

| Status | Description |
|---|---|
| Disconnected (Login Failed) | The username, password or crypto key (3DES) entered is wrong. |
| Disconnected (Duplicate Connection) | Another GV-ASManager is connecting with the GV-AS Controller. |
| Disconnected (Hardware Error) | The Controller ID entered is wrong. Or GV-AS Controller errors occur. |